EAGLE
North Carolina
Office of the State Controller
Enhancing Accountability in Government through Leadership and Education

EAGLE Program

Guidance Manual

OVERVIEW OF THE EAGLE PROGRAM APPROACH

PAGE

APPENDICES

Note: The Financial templates linked in the Appendices section are examples of how to complete the templates. The Compliance templates are blank templates; please refer to the compliance case study located on the EAGLE Site.

1. INTRODUCTION

1.1 WHAT IS EAGLE?

The current business environment has significantly heightened the expectations of stakeholders regarding the adequacy and effectiveness of an organization's internal controls that support its financial, operational, and compliance objectives. Effective internal controls are the foundation for managing risk and creating a safe and sound operating environment. While emphasis in the past has been on regulating for-profit public companies, internal controls are becoming more important in the Government and Not-for-Profit sectors. This is driven primarily by inquiries from stakeholders including the federal government, Compliance and Internal Audit functions, and bond rating agencies (North Carolina currently has a Triple-A Bond Rating) as well as enhanced public accountability to key stakeholders, namely taxpayers of the State of North Carolina.

Enhancing Accountability in Government through Leadership and Education (EAGLE) is the State's internal control program that was established by the Office of the State Controller (OSC) to meet the requirements of House Bill 1551, Chapter 143D "State Governmental Accountability and Internal Control Act."

Refer to the EAGLE website at http://www.osc.nc.gov/eagle/ for an excerpt from House Bill 1551.

The North Carolina statewide internal control program defines the vision of an effective system of internal controls for North Carolina State government.

The statewide internal control framework is supported by:

- Enabling Legislation - ensuring that the vision of effective controls is properly applied
- Standards and Policies - expanding existing policies and promulgating new standards to fully implement the vision of effective internal controls
- Communication and Training - connecting with State Government and relaying the vision
- Self-Assessment of Current Environment - assessing risk and identifying areas for improvement
- Compliance Monitoring - assisting North Carolina State Government in proactively mitigating risks
- Everyone's Responsibility - An effective system of internal control can only be preserved by the diligence of every person involved in North Carolina State Government.

1.2 WHAT IS THE PURPOSE OF EAGLE?

The purpose of the EAGLE Program is not only to establish adequate internal control but also to increase fiscal accountability within State government.

To accomplish the requirements of House Bill 1551, the OSC will:

1. Establish comprehensive standards, policies, and procedures to serve as a foundation for strong and effective internal controls

2. Make appropriate education efforts to inform state agencies of these standards, policies, and procedures which shall include training courses, manuals and other information resources to promulgate a strong and effective system of internal control over financial reporting and compliance in state agencies

Additionally, the OSC will provide ongoing assistance and monitoring to support State agencies in their efforts. Via the EAGLE website, located on the website of the Office of the State Controller (http://www.osc.nc.gov/eagle/), the OSC will provide general communication concerning the EAGLE Program as well as resources including the internal control guidance manual, assessment templates, policies and procedures, calendar, contact information, and responses to Frequently Asked Questions (FAQ) to assist State agencies in performing their assessments. The OSC may also be available to assist State agencies on site.

1.3 PROGRAM EXPECTATIONS AND TIMELINE

Agency Expectations

Under the EAGLE Program, each agency will be required to perform an annual assessment of internal control. By completing this assessment, agencies will benefit by: 1) identifying risks and compensating controls that reduce the possibility of material misstatements and misappropriation of assets; 2) identifying compliance requirements and correlating controls for federal programs/grants; and 3) recognizing opportunities to increase efficiency and effectiveness in business processes and operations.

Each State agency will be asked to upload to the EAGLE website all required internal control assessment documents as well as all significant changes, issues, corrective actions and resolutions. The EAGLE website and download/upload instructions will be discussed further in Chapter 9.

1.4 GUIDANCE MANUAL AND TRAINING PROGRAM

This manual has been prepared to assist State agencies in establishing standards, policies, and procedures necessary for an effective internal control system. This manual serves as a supplement to the one-day training program and is designed as a flexible set of principles, guidelines, and tools that can be followed to help each agency in performing its own internal control assessment. We will also have some internal control training throughout the year which will be available to any state employee.

2. OVERVIEW OF INTERNAL CONTROLS

2.1 INTRODUCTION

One commonly used and understood framework for evaluating internal controls over financial reporting is contained in the report of The Committee of Sponsoring Organizations of the Treadway Commission (COSO). COSO is a voluntary organization originally formed in 1985 to sponsor the National Commission on Fraudulent Financial Reporting, an independent initiative that studied and developed recommendations for the causal factors that can lead to fraudulent financial reporting. The National Commission was jointly sponsored by five major professional associations in the United States: the American Accounting Association, the American Institute of Certified Public Accountants, Financial Executives International, the Institute of Internal Auditors, and the National Association of Accountants (now the Institute of Management Accountants). The Commission was wholly independent of each of the sponsoring organizations and included representatives from industry, public accounting, investment firms and the New York Stock Exchange.

The COSO report, *Internal Control—Integrated Framework*, established a broad definition of internal control extending to all objectives of an organization.

2.2 DEFINITION OF INTERNAL CONTROL

In order to assess an organization's internal control environment, one must first identify the criteria against which the assessment will be made. Therefore, it is important to appropriately identify internal controls early in the evaluation process. The COSO report contains the most widely accepted definition of internal control.

Internal control is broadly defined as a process, affected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following three COSO categories:

- Reliability of financial reporting - This is related to the preparation of reliable published financial statements, including interim and condensed financial statements, such as the CAFR, reported publicly.
- Compliance with applicable laws and regulations - This deals with complying with those laws and regulations to which the entity is subject.
- Effectiveness and efficiency of operations - This addresses an entity's basic business objectives, including performance and profitability goals and safeguarding of resources.

In assessing the design and operating effectiveness of internal controls over financial reporting (ICFR), under the COSO framework, management also considers the five components of internal control as depicted in the COSO "Cube". If designed and operating effectively, controls within these five components in totality provide a framework for internal control.

Five Components of COSO

- Control Environment

  The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure. Control environment factors include:

  - Integrity, ethical values and competence of the entity's people,
  - Management's philosophy and operating style,
  - Commitment to competence,
  - Organizational structure and assignment of authority and responsibility,
  - Board of Directors and/or audit committee participation in governance and oversight, and
  - Human resources' policies and practices.

- Risk Assessment

  Every entity faces a variety of risks from external and internal sources that must be assessed. A precondition to risk assessment is establishment of objectives, linked at different levels and usually internally consistent. Risk assessment is the identification and analysis of relevant risks to achievement of the objectives, forming a basis for determining how the risks should be managed. Because economic, industry, regulatory and operating conditions will continue to change, mechanisms are needed to identify and deal with the special risks associated with change. Some factors to consider in understanding the risk assessment process are:

  - Whether entity-level objectives have been established and communicated,
  - Whether a risk assessment process, including estimating the significance of risks, assessing the likelihood of their occurrence, and determining needed actions, has been established,
  - Whether mechanisms are in place to anticipate, identify, and react to changes that may have a dramatic and pervasive effect on the entity, and

- Whether the accounting department has processes in place to identify significant changes in generally accepted accounting principles promulgated by relevant authoritative bodies and/or changes in the operating environment, including regulatory changes.

- Control Activities

  Control activities are the policies and procedures that help determine if management directives are carried out. They help facilitate the necessary actions required to address risks to achievement of the entity's objectives. Control activities occur throughout the organization, at all levels and in all functions. They include a range of activities as diverse as approvals, authorizations, verifications, reconciliations, reviews of operating performance, security of assets and segregation of duties. In understanding control activities at the entity level, some factors to consider are:

  - Whether the necessary policies and procedures exist with respect to each of the entity's activities,
  - The extent to which controls called for by policy are being applied,
  - Whether management has clear objectives in terms of budget, profit, and other financial and operating goals, and whether these objectives are clearly written, communicated and monitored,
  - Whether planning and reporting systems are in place to identify variances from planned performance and communicate variances to appropriate levels of management,
  - Whether the appropriate level of management investigates variances and takes appropriate timely and corrective action,
  - To what extent duties are divided logically through appropriate set up of information technology applications,
  - Whether adequate safeguards are in place to prevent unauthorized access to or destruction of documents, records, and assets, and
  - Whether access security software, operating system software, and/or application software is used to control access to data and programs.

- Information and Communication

  Pertinent information must be identified, captured and communicated in a form and timeframe that enables people to carry out their responsibilities. Information systems produce reports, containing operational, financial and compliance-related information, that make it possible to run and control the business. They deal not only with internally generated data, but also information about external reporting. Effective communication must also occur in a broader sense, flowing down, across and up the organization. All personnel must receive a clear message from top management that control responsibilities must be taken seriously. They must understand their own role in the internal control system, as well as how individual activities relate to the work of others. They must have a means of communicating significant information upstream. There also needs to be effective communication with external parties, such as customers, suppliers, regulators and shareholders. In

gaining an understanding of information and communication at the entity level, some factors to consider are:

- Whether the information system provides the necessary reports to management to assess the entity's performance,
- To what extent information systems are developed or revised based on a strategic plan that is interrelated with the entity's overall information systems, and is responsive to achieving the entity-level and process/application level objectives,
- Whether management commits the appropriate human and financial resources to develop the necessary information systems,
- How management ensures and monitors user involvement in the development and testing of programs,
- Whether a disaster recovery plan has been established for all primary data centers,
- Whether management communicates employees' duties and control responsibilities in an effective manner,
- Whether communication channels have been established for people to report suspected improprieties, and
- Whether the agency is subject to monitoring and compliance requirements imposed by legislative and regulatory bodies.

- Monitoring

  Internal control systems need to be monitored (a process that assesses the quality of the system's performance over time). This is accomplished through ongoing monitoring activities, separate evaluations or a combination of the two. Ongoing monitoring occurs in the course of operations. It includes regular management and supervisory activities, and other actions personnel take in performing their duties. The scope and frequency of separate evaluations will depend primarily on an assessment of risks and the effectiveness of ongoing monitoring procedures. Internal control deficiencies should be reported upstream, with serious matters reported to top management and the board (if applicable).

In September 2004, COSO issued the *Enterprise Risk Management – Integrated Framework.* The new framework addresses internal control within enterprise risk management. Internal control is encompassed within and is an integral part of enterprise risk management. Enterprise risk management is broader than internal control, however, expanding and elaborating on internal control to form a more robust conceptualization focusing more fully on risk. The new framework expands from three objectives to four and expands from five components into eight (it also changes one of the components from "Control Environment" to "Internal Environment"). The new objective is "Strategic" which deals with an organization's high-level goals, aligned with and supporting its mission. The additional components are "Objective Setting", "Event Identification" and "Risk Response".

Internal Control – Integrated Framework remains in place for organizations and others reviewing internal control on a standalone basis and should continue to be used. However, in the future, organizations may decide to look to the enterprise risk management framework both to satisfy their internal control needs and to move toward a more robust risk management process.

2.3 COBIT

While COSO is commonly accepted as the internal control framework for organizations, COBIT is the accepted internal control framework for the information technology (IT) environment. Control Objectives for Information and related Technology (COBIT) was first released by the Information Systems Audit and Control Foundation (ISACF) in 1996 and has been updated to include current IT governance principles and emerging international, technical, professional, regulatory and industry specific standards. The resulting control objectives have been developed for application to organization-wide information systems. Now in Edition 4.1, COBIT is intended to meet the multiple needs of management by bridging gaps between business risks, control needs and technical issues.

The COBIT framework is based on the following principle:

> To provide the information that the organization requires to achieve its objectives, the organization needs to invest in and manage and control IT resources using a structured set of processes to provide the services that deliver the required organization information.

The COBIT framework identifies 34 IT processes and an approach to control over these processes. It provides a generally applicable and accepted standard for sound IT security and control practices to support management's needs in determining and monitoring the appropriate level of IT controls for their organizations.

Four Sections of the COBIT 34 IT Processes

The COBIT framework is structured in four principle domains. Each domain includes unique processes which sum to the 34 IT processes discussed above. This structure serves as a process model for an enterprise to manage IT activities. Those IT activities in bold italics are related to financial reporting processing.

- **Plan and Organize (PO)**

  This domain covers strategy and tactics, and concerns the identification of the way IT can best contribute to the achievement of the business objectives. The realization of the strategic vision needs to be planned, communicated and managed for different perspectives. A proper organization as well as technological infrastructure should be put in place. This domain addresses the following processes:

PO1 Define a Strategic IT Plan
PO2 Define the Information Architecture
PO3 Determine Technological Direction
PO4 Define the IT Processes, Organization and Relationships
PO5 Manage the IT Investment
PO6 Communicate Management Aims and Direction
PO7 Manage IT Human Resources
PO8 Manage Quality
PO9 Assess and Manage IT Risks
PO10 Manage Projects

- **Acquire and Implement (AI)**

  To realize the IT strategy, IT solutions need to be identified, developed or acquired, as well as implemented and integrated into the business process. In addition, changes in and maintenance of existing systems are covered by this domain to make sure the solutions continue to meet business objectives. This domain addresses the following processes:

  AI1 Identify Automated Solutions
  AI2 Acquire and Maintain Application Software
  AI3 Acquire and Maintain Technology Infrastructure
  AI4 Enable Operation and Use
  AI5 Procure IT Resources
  AI6 Manage Changes
  AI7 Install and Accredit Solutions and Changes

- **Deliver and Support (DS)**

  This domain is concerned with the actual delivery of required services, which includes service delivery, management of security and continuity, service support for users, and management of data and operational facilities. It addresses the following processes:

  DS1 Define and Manage Service Levels
  DS2 Manage Third-Party Services
  DS3 Manage Performance and Capacity
  DS4 Ensure Continuous Service
  DS5 Ensure Systems Security
  DS6 Identify and Allocate Costs
  DS7 Educate and Train Users
  DS8 Manage Service Desk and Incidents
  DS9 Manage the Configuration
  DS10 Manage Problems
  DS11 Manage Data
  DS12 Manage the Physical Environment
  DS13 Manage Operations

- **Monitor and Evaluate (ME)**

  All IT processes need to be regularly assessed over time for their quality and compliance with control requirements. This domain addresses performance management, monitoring of internal control, regulatory compliance and governance. It addresses the following processes:

  ME1 Monitor and Evaluate IT Performance
  ME2 Monitor and Evaluate Internal Control
  ME3 Ensure Compliance with External Requirements
  ME4 Provide IT Governance

2.4 RESPONSIBILITY FOR INTERNAL CONTROL SYSTEM

Responsibility for the establishment and monitoring of the internal control system resides with the following personnel:

- Management – The chief executive officer is ultimately responsible and should assume "ownership" of the system. More than any other individual, the chief executive sets the "tone at the top" that affects integrity, ethics, and other factors of a positive control environment. Also of significance are the financial officers and their staff, whose control activities cut across, as well as up and down, the operating and other units of an agency.
- Internal Auditors – Internal auditors play an important role in evaluating the effectiveness of control systems and contribute to ongoing effectiveness. Because of organizational position and authority in an entity, an internal audit function often plays a significant monitoring role.
- Other Personnel – Internal control is, to some degree, the responsibility of everyone in an organization and, therefore, should be an explicit or implicit part of everyone's job description. Virtually all employees produce information used in the internal control system or take other actions needed to affect control. Also, all personnel should be responsible for communicating upward problems in operations, noncompliance with the code of conduct, or other policy violations or illegal actions.

2.5 CONCLUSION

This manual focuses on controls over financial reporting and compliance. There are many similarities and common considerations among controls related to financial reporting and controls related to compliance with laws and regulations as well as effectiveness and efficiency of operations.

The following chapters of the manual are designed to assist management by providing a methodology for transforming the COSO and the COBIT conceptual frameworks into a detailed, meaningful evaluation of internal controls over financial reporting.

3. TOP-DOWN, RISK-BASED APPROACH

3.1 INTRODUCTION

Definition

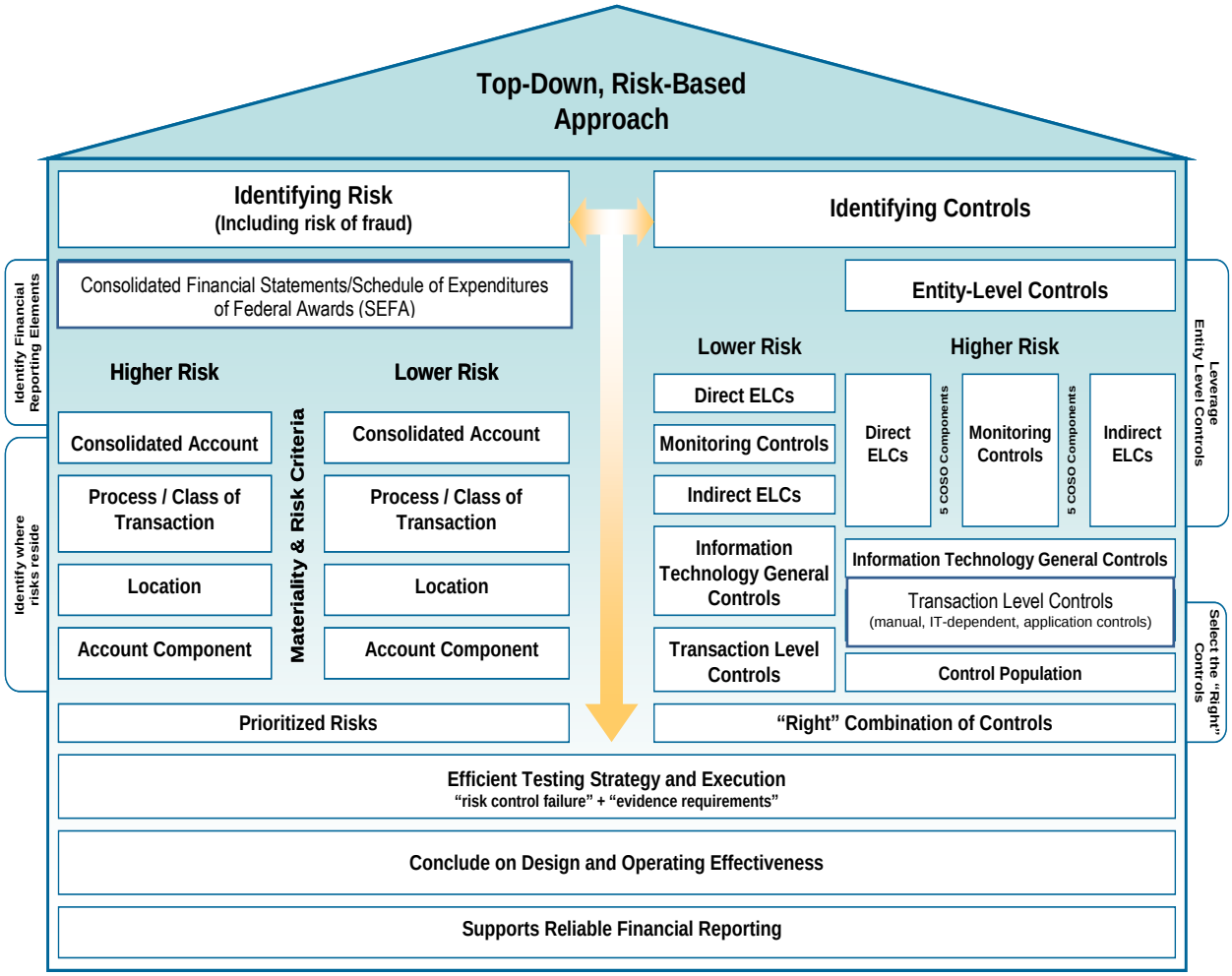
A top-down, risk-based approach is an approach to conducting an internal control assessment that identifies the risks related to reliable financial reporting and compliance, the combination of controls that effectively and efficiently addresses those risks, and evaluates the evidence necessary to conclude on the effectiveness of such controls. The approach rests on the premise that not all risks are equal, and management's effort should be tailored according to the nature (i.e., likelihood and magnitude) of the identified level of risk.

Overview

The goal of the assessment process required by the EAGLE Program is to determine whether there is a reasonable possibility that the agency's internal control over financial reporting (ICFR) and compliance will fail to prevent or detect, in a timely manner, a material misstatement in the financial statements and disclosures or noncompliance with laws and regulations. This goal can be achieved more efficiently with a top-down, risk-based approach. The top-down, risk-based approach represents a thought process – a management perspective – that focuses on the organization as a whole and drives allocation of more resources to the areas of highest risk to reliable financial reporting and compliance with applicable laws and regulations. To help sharpen management's focus on areas of greatest risk, the top-down, risk-based approach encourages management to identify those accounts or programs/grants, and business processes or compliance requirements which have a higher likelihood of posing a material weakness or noncompliance, and to adjust the nature, extent, and timing of control testing efforts in those particular areas. Numerous benefits of this process include: focusing more effort on areas of higher financial reporting or compliance risk; reducing the effort expended on lower risk areas; and leveraging strong entity-level controls to reduce the amount of detailed transaction-level testing.

Model Diagram

To help explain the top-down, risk-based concept, a "house" diagram (as shown on the following page) can be used to depict the elements management should consider in assessing internal controls.



The 3 main activities that serve as the foundation of the "house" are:

1. Risk identification (Chapter 4)
2. Controls identification (Chapters 5 and 6)
3. Execution and evaluation (Chapters 7)

The risk identification activity, or "risk assessment," involves identifying and assessing material financial reporting and compliance risks. The controls identification activity involves defining the "right" combination of controls to sufficiently address the risks identified in the risk assessment. Once the controls have been selected, the model is supported by a well-designed execution plan and evaluation that includes a testing strategy for identified controls that supports management's assessment.

These activities, when undertaken together, provide management with a path to achieving reasonable assurance regarding the reliability of its financial reporting and compliance with applicable laws and regulations. The entire model rests on the premise of prioritized areas of risk and the "right" combination of internal controls. One of the critical success factors in

implementing a top-down, risk-based approach is the availability of information and data pertaining to financial reporting and compliance elements. Organizations that have a clear understanding of how their financial reporting and compliance elements are supported by relevant information systems are generally better positioned to successfully implement this guidance. Each of these activities is necessary for successful implementation of the top-down, risk-based approach and is described in further detail below.

3.2 RISK IDENTIFICATION

Risk identification is a continuous element in planning the overall assessment and is the cornerstone to an efficient and effective internal control program. Management should use its knowledge and understanding of the business, its organization, operations and processes to consider the sources and potential likelihood of misstatement in financial reporting and noncompliance with laws and regulations and identify those sources that could result in a material misstatement to the financial statements or noncompliance. Included in this understanding is consideration for the generally accepted government auditing standards (GAGAS) that apply to its agency and the related risks to fair presentation of the financial statements and compliance with laws and regulations.

Successful top-down risk assessments often identify the accounts or programs/grants, and business processes or compliance requirements with a greater likelihood and larger magnitude of potential material financial misstatements or noncompliance. As one of the first steps in analyzing the potential risk of a material misstatement at the consolidated financial statement account level or Schedule of Expenditures of Federal Awards at the program/grant level, the risk assessment helps management determine, using both quantitative and qualitative risk factors, which accounts or programs/grants pose a greater risk of having a material financial misstatement or noncompliance with a federal requirement.

In conjunction with assessing the consolidated financial statement account risk, management may find it helpful to assess the relevance of each of the financial statement assertions related to each account (e.g., existence and occurrence; completeness; valuation and measurement/allocation; rights and obligations; and presentation and disclosure - Appendix 4.2C). This will focus management's attention on identifying specific areas of risk within an account.

In conjunction with assessing the Schedule of Expenditures of Federal Awards, management may find it helpful to review the relevance of each compliance requirement within the Compliance Internal Control Guidance (Appendix 4.2D) related to each program/grant. This will also focus management's attention on identifying specific areas of risk with a program/grant.

Business processes and compliance requirements can be assessed in much the same manner. Documenting the level of risk associated with business processes or compliance requirements can allow management to study the accounts or programs to determine what specific business processes or compliance requirements are driving the higher-risk activities. Management can then focus its efforts accordingly.

The following discussions outline some of the key areas within risk assessment activities where management may identify opportunities to focus efforts on specific risks identified through the process.

1. Materiality Decisions
   Materiality thresholds are an important consideration for management's assessment. While overall, materiality is, in large part, a quantitative consideration based on key financial measures (e.g., revenues or expenses), it is also important to consider inherent risks of misstatement, the expectations of key stakeholders, and other qualitative factors. The key insight here is that management should challenge whether the levels of materiality used to identify in-scope financial reporting and program/grant elements and risks appropriately reflect both **quantitative** and **qualitative** factors.

2. Identification of Financial Reporting and Compliance Elements
   Typically, management breaks down consolidated financial statement line items and disclosures into individual **financial reporting elements** to determine those that are material to the organization. This exercise is very important as individual consolidated accounts can be made up of many components, each with different levels of materiality and risk. This is where management exercises judgment and uses its knowledge of the business to determine risks specific to the organization. For example, an account may be of high monetary value yet still be determined to be low risk due to the low probability of a material misstatement associated with the account. On the other hand, there are some accounts that might be of low monetary value, and yet should be included in scope due to their higher risk of material misstatement based on qualitative factors.

   For the compliance element, the Schedule of Expenditures of Federal Awards (SEFA) identifies each program/grant per the Catalog of Federal Domestic Assistance (CFDA) number to determine those that are material to organization. Program/grants that are part of a cluster or have similar requirements may be grouped. Programs with the same CFDA number that are listed separately on the SEFA due to the American Recovery and Reinvestment Act (ARRA) may also be grouped. Management should exercise judgment and use its knowledge of the business to determine risks specific to each program/grant.

3. Development of Financial Reporting and Program/Grant Risk Assessment Criteria
   Once "in scope" risks are identified, management should prioritize these risks. This prioritization will be important for future activities such as facilitating better risk-based control identification and developing testing strategies. Leading practices indicate that once financial reporting elements and related assertions have been identified, management should develop customized risk assessment criteria, including the risk of fraud. Management should consider fraud risk factors at the account and program/grant level as well as the process and compliance requirement level as part of its approach to evaluating internal controls. The likelihood of fraud occurring generally increases when one or more fraud risks are present, particularly in an environment where significant

pressure exists to meet financial or operational targets. Refer to Chapter 10 for more information on Fraud concepts.

Risk rating and prioritization are judgmental processes and, therefore, highly dependent on the experiences of participants involved in the process. Validating risk criteria and prioritization outcome is crucial. Refer to Chapter 4 for recommended criteria for the risk assessment.

4. Consideration of Significant Processes/Compliance Requirements
   To understand risks within financial reporting or compliance elements, management is encouraged to identify the major classes of transactions affecting those elements and related significant processes or compliance requirements. By "significant processes" and "compliance requirements," we mean those that materially affect the financial reporting or compliance elements. Different types of transactions have varying levels or risk and likelihood of errors. For example, classes of transactions might be routine and involve frequently recurring financial data. Other classes of transactions might be non-routine or involve estimation or numerous judgments and assumptions and, therefore, represent higher risk (significant processes and compliance requirements will be discussed further in Chapter 5).

3.3 CONTROLS IDENTIFICATION

The controls side of the "house" has to do with selecting the "right" combination of controls that adequately addresses the organization's risks. The word "right" is used because management has the flexibility to consider efficiency with which controls can be evaluated when determining which combination of controls should be selected for testing as part of its assessment. Typically, management first considers entity-level controls (ELCs) and then transaction-level controls (TLCs). The premise behind this approach is that, in general, ELCs that are pervasive in nature may be more efficient and effective in addressing risk across the organization. Information technology (IT) also plays a vital role in an organization's system of internal control and impacts an organization's financial reporting processes and, by extension, its internal control program. As such, management must also consider IT controls when determining the "right" combination of controls.

Entity-Level Controls

Entity-Level Controls (ELCs) set the tone of an organization's overall system of internal control and generally have a wide scope impact on the achievement of the organization's objectives for internal control. Management's evaluation process must include not only controls over particular areas of financial reporting and compliance risk, but also the entity-wide and other pervasive elements of internal control defined by its selected control framework. Therefore, an effective system of internal control includes a balance of ELCs and Transaction-Level Controls (TLCs) that work in combination.

ELCs are organized in categories consistent with the COSO framework: monitoring, information and communication, control activities, risk assessment and control environment. In

the past, ELCs have been under-leveraged. Now, however, leading organizations realize they can test fewer TLCs when effectively utilizing ELCs. When ELCs are operating effectively, management can enjoy a higher level of confidence that the TLCs will continue to function effectively over time.

There are three primary types of ELCs:

1. Indirect controls are those controls that are cross-functional and which affect the achievement of the organization's control objectives in indirect, but important ways. *Examples include such control environment controls as a code of conduct or code of ethics as well as communication and training efforts.*

2. Direct controls are controls that operate directly at the process, transaction, or application level and are designed to timely prevent or detect material misstatements in one or more financial reporting elements. *Examples include period-end financial reporting activities such as monthly reconciliations and analytics such as margin or variance analyses.*

3. Monitoring controls are those that monitor the effectiveness of other controls and identify possible breakdowns among lower-level controls, though not in a manner that would, by themselves, sufficiently address the risk that material misstatements in financial reporting and compliance will be timely prevented or detected. *Examples include activities of the internal audit function.*

An organization that can identify and evaluate direct entity-level controls sensitive enough to detect or prevent material financial misstatements and noncompliance may be able to reduce testing at a detailed transaction level, especially in lower risk areas. While most ELCs are not designed to have the necessary precision and direct relationship to accounts and assertions to, by themselves, address the risk, management should consider the following questions when determining the level of precision:

- Is the control sensitive enough to detect a significant error, deficiency, or fraud?
- Is the control designed and performed effectively? Is the control performed frequently enough?
- Is the control reliable and repeatable? Is the control appropriately reviewed?
- Is the reviewer of the control competent and well-trained?

In most cases, it will be necessary to identify a combination of ELCs and TLCs to gather sufficient evidence that controls adequately address a particular risk. However, in general, as ELCs increase in precision and more directly relate to specific financial reporting and compliance elements and assertions, the more reliance management may be able to place on them. This may result in management needing less evidence to support the operating effectiveness of certain TLCs that operate in combination with ELCs to address risks related to specific financial reporting and compliance elements and assertions.

Information Technology Controls

Information Technology (IT) controls consist of the following three types, all of which are needed to confirm complete and accurate information processing as part of the internal control assessment:

1. Application Controls
2. IT-dependent Manual Controls
3. IT General Controls

The following discussions provide further details on each type:

Application Controls

Application controls (also known as automated process controls) are configurable controls within a business application designed to prevent or detect and correct errors or anomalies in the inputs, processes, or outputs. In addition, application controls consist of controls designed around interfaces between business applications and access to specific functionality, such as the setup of the chart of accounts or the configuration of three-way match. In other words, an application control is a specific process control that is dependent upon a computer application to function.

IT-Dependent Manual Controls

IT-dependent manual controls are performed by an individual who relies on some type of automated output. When testing IT-dependent controls, the tester typically performs two separate tests: the IT portion, to validate the accuracy and completeness of the system-generated report, and the manual portion, to test the effectiveness of the manual portion of the control the same way they would test any other manual control.

IT General Controls (ITGCs)

ITGCs set the tone within the IT control environment by supporting the functioning of application controls and IT-dependent manual controls. ITGCs are typically broken out into the following three areas:

- Access to programs and data (e.g., The process of granting access to an organization's data to modify, delete, or enhance it.)
- Program change and development (e.g., Looking at the software development life cycle and asking such questions as who modifies the programs, what are the controls surrounding those changes, is there a rigorous change management process in place?)
- Computer operations (e.g., How does the organization run its IT department?)

Included in the family of Information Technology controls are End-user computing controls. End-user computing generally involves the use of department-developed spreadsheets and databases, which are frequently used as tools in performing daily work. To the extent these spreadsheets are in place, they are an extension of the IT environment and results generated from them may, in assessing their impact, have an effect on the organization's financial statements. Controls around End-user computing will be discussed further in Chapter 5.

A top-down, risk-based approach to testing IT controls starts with first determining those applications and associated automated or IT-dependent manual controls that are important to the assessment of internal control, and then determining the ITGCs that are relevant to those applications and associated automated or IT-dependent manual controls. Thus, if it is determined that no automated or IT-dependent manual controls are in scope for a given account or process, management need not test the related ITGCs.

Transaction-Level Controls

Transaction-level controls include:

1. Manual controls
2. IT-dependent manual controls
3. Application controls
4. End-user computing controls

Management identifies only those transaction-level controls that address identified risks and has the discretion to not identify controls that are not important to achieving the objectives of internal controls. In addition, in identifying the "right" combination of controls, management has the discretion to select controls for which evidence of operating effectiveness can be attained more efficiently.

Refer to Chapter 5 for further detail on Introduction to Processes and Controls. Refer to Chapter 6 for further detail on Documentation of Processes and Controls.

3.4 EXECUTION AND EVALUATION

After documenting processes and identifying the "right" combination of controls, a testing strategy may be designed to focus efforts on those controls that have been designed to prevent or detect errors of the highest risk processes or compliance requirements.

"Testing" refers to the procedures performed to obtain evidence about the operating effectiveness of controls. The evidence that management evaluates comes from direct test of controls, ongoing monitoring, or a combination of both. Management is in the best position to determine the character and quality of evidence required to support its assessment about the operating effectiveness of internal controls.

Determining the nature, extent, and timing of control testing is a matter of management judgment. Leading organizations determine their testing strategy considering the risk of control failure or the level of risk. There is no requirement to test every control in a process. What to test is a matter of management judgment.

That judgment will depend on considerations related to the following:

1. What to test (whether the controls reside among transaction-level, entity-level, or both).
2. How to test, relates to the level of evidence needed to adequately assess the operating effectiveness of the control.
3. When to test, depending on the nature of the control and the judgment required.

It is important to highlight here that agencies should focus on and test only those controls (critical controls) that are needed to adequately address those risks that could lead to a material misstatement in the financial statements or noncompliance with law and regulations. Further, as the assessed level of risk increases, agencies should vary the nature of evidence from ongoing monitoring to direct testing of controls and/or by adjusting the period of time covered by direct testing. Once testing of internal controls has been completed, management completes its assessment of internal control over financial reporting and compliance.

Refer to Chapter 7 for further detail on Testing Theory and Strategy. Refer to Chapter 9 for further detail on Agency Self-Assessment.

3.5 ROADMAP FOR IMPLEMENTATION OF A TOP-DOWN, RISK-BASED APPROACH

While the discussion above focuses on three high-level activities involved in implementing a top-down, risk-based approach to internal controls evaluation, the following depicts a more detailed roadmap for the evaluation of internal controls. Each activity listed in this diagram is discussed in more detail in subsequent chapters (4-9).

Procedures to perform the Top-Down, Risk-Based Approach

Financial Risk Assessment			Compliance Risk Assessment		
Template 01 –A	Assess risk at the financial statement account level.	☐	**Template 01 –B**	Assess risk for the program/grant.	☐
	Assess risk at the financial statement process level.	☐			
	Assess risk at the financial statement location level, if applicable.	☐		Assess risk for each requirement.	☐
Risk Assertion Guidance	Review Financial Statement Assertions Guidance	☐	**Compliance Guidance**	Review Compliance Internal Control Guidance	☐
Identify Controls					
Template 02	**Narrative -** Document the applicable processes/compliance requirements.				☐
Template 03	**Walkthrough -** Walk through the applicable processes/compliance requirements.				☐
Template 04	**Service Provider/Reliance on Others** - Identify and document reliance on others.				☐
Template 05	**Risk and Control Matrix** - Identify the "right" combination of controls.				☐
Evaluate and Execute					
Template 06	**Test Plan** - Determine the testing selections for applicable controls.				☐
Template 06	**Test Leadsheet** - Perform testing of selected controls.				☐
Template 07	**Issue Summary Log** - Document issues and management's response.				☐
Performance Measures					
Template 08	**General Accounting**				☐
Template 09	**Student Financial Aid (Community Colleges only)**				☐
Template 10	**Federal Grants**				☐
Template 11	**Procurement**				☐
Internal Control Certification					
Internal Control Certification Letter Due 7/31/20XX	Each President or Chief Executive Officer and Chief Financial Officer shall annually certify, in a manner prescribed by the State Controller, that the college has in place a proper system of internal control.				☐

4. IDENTIFYING RISK

4.1 INTRODUCTION

Top-down risk assessments are performed to identify the risks related to reliable financial reporting and compliance with applicable laws and regulations. It is an approach that identifies the combination of controls that addresses those risks and evaluates evidence necessary to conclude on the effectiveness of such controls. In analyzing the potential risk of a material misstatement at the consolidated financial statement account level or noncompliance with a federal requirement, the risk assessment helps management to determine, using both quantitative and qualitative risk factors, which accounts or compliance requirements pose a greater risk of having a material financial misstatement or noncompliance. The approach rests on the premise that not all risks are equal, and management's effort should be tailored according to the nature of the identified level of risk.

The risk assessment activities involve identifying and assessing material financial reporting and program/grant compliance risks. Management uses its knowledge and understanding of the business, its organization, operations, and processes to consider the sources and potential likelihood of misstatement in financial reporting and program/grant compliance requirements and identifies those sources that could result in a material misstatement to the financial statements or noncompliance with laws and regulations. Internal and external risk factors impacting the business, including the nature and extent of any changes in those risks, may give rise to financial reporting and compliance risks. Financial reporting risks may also arise from sources such as the initiation, authorization, processing and recording of transactions and other adjustments that are reflected in the financial reporting elements. Management's evaluation of financial reporting and compliance risks should also consider the vulnerability of the agency to fraudulent activity (for example, fraudulent financial reporting, misappropriation of assets, and corruption) and whether any of those exposures could result in a material misstatement to the financial statements or noncompliance with a federal requirement.

Financial Risk Assessment

Assessment of financial reporting risks begins with the identification of financial reporting elements; specifically, the individual accounts, notes and disclosures that make up the consolidated financial statements. The agency defines the material financial reporting elements and then prioritizes them using risk assessment criteria. Next, the agency will identify the processes relating to the material accounts, and determine the locations where the processes are performed, if applicable. Agencies will then gain an understanding of what could go wrong in those processes (which may differ by location) to help further define the financial reporting risk. Finally, the agency will prioritize the financial reporting risks. This process is facilitated by the use of management's judgment to determine what is material to the consolidated financial statements and considers the characteristics of individual financial reporting elements and the likely sources of misstatement within the significant processes within an agency.

Components of Financial Risk Assessment

The financial statement risk assessment is composed of four components:

1. Account risk - Account risk considers the underlying risk associated with the financial statement account, from its size and materiality to the complexity and subjectivity of transactions it represents. (Note: Accounts represent the financial statement line items. Agencies may refer to these as Captions.)
2. Process risk - Process risk takes the information gained in the Account risk stage and applies it to the individual processes that constitute the financial statement accounts. This provides a more detailed analysis that is later used to assist in the determination of the organization's testing effort.
3. Location risk - Location risk helps management to understand which locations represent the highest risk for each financial statement account and consequently require the most effort to test.
4. Financial Statement Assertion Guidance - The Financial Statement Assertion Guidance document focuses on the risk associated with the five financial statement assertions for each of the financial statement accounts.

Each of these components of risk uses a series of quantitative and qualitative factors as part of the risk assessment. Some of these are relatively simple to obtain, such as the size and composition element of the Account Risk criteria. Others require management to exercise judgment in defining the criteria for High, Moderate and Low risk and the application of these criteria to the accounts.

Compliance Risk Assessment

Assessment of the federal compliance requirement risks begins with Schedule of Expenditures of Federal Awards (SEFA) report. The agency indentifies the Federal Programs/Grants and then prioritizes them using the risk assessment criteria. Next, the agency will identify the compliance requirements relating to the programs/grants and assess the risk of what could go wrong with each of these requirements. Finally, the agency will prioritize the compliance risks.

Components of Compliance Risk Assessment

A compliance risk assessment is composed of two components:

1. Program/Grant Risk - Program/Grant Risk considers the underlying risk associated with each of the programs/grants, from its size and composition to the complexity and other inherent risk.
2. Requirement Risk - Requirement risk takes the information gained in the program/grant risk stage and applies it to the individual requirements of each program/grant.

Each of the components of risk uses a series of quantitative and qualitative factors as part of the risk assessment. Some of these are relatively simple to obtain through Circular A-133

(Compliance Supplement published by the Federal Office of Management and Budget), while others will require further research.

Impact on Information Technology

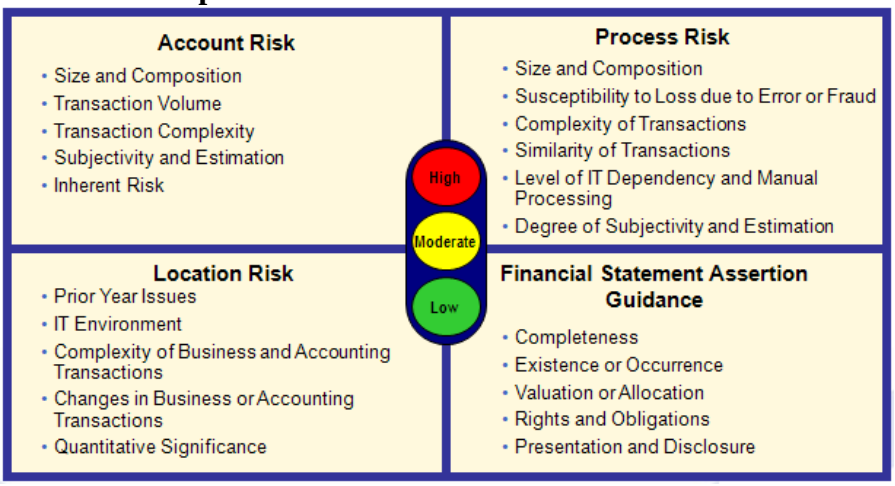
Application scoping is an output of the risk assessment process, and IT general controls, IT application controls, and IT-dependent manual controls serve as a large part of an entity's control environment. These will be discussed in later chapters in more detail.

4.2 PERFORMING THE RISK ASSESSMENT

Financial Risk Assessment

The financial statement risk assessment is based around the four risk components previously introduced. Criteria are developed for each component, and are based around risk factors that can be tailored by the organization. Information to develop the risk assessment criteria is obtained from a number of sources to understand the organizational structure, strategy, management, fraud prevention and operational issues faced by the organization. Each criterion is developed with key stakeholders and is then validated with senior personnel.

Components of the Financial Risk Assessment



The risk criteria discussed below for the four components are recommended by the Office of the State Controller to be used by the State agencies in conducting their risk assessments.

Assessing Account Risk

In performing the risk assessment, the agency first identifies the financial reporting elements which include the financial statement accounts, notes and disclosures that will form the basis of the financial reporting risk profile. The agency can use the following to facilitate the identification of the financial reporting elements:

- The consolidated Statement of Net Assets (Balance Sheet) and Statement of Revenues, Expenses and Changes in Net Assets (Income/Operating Statement)

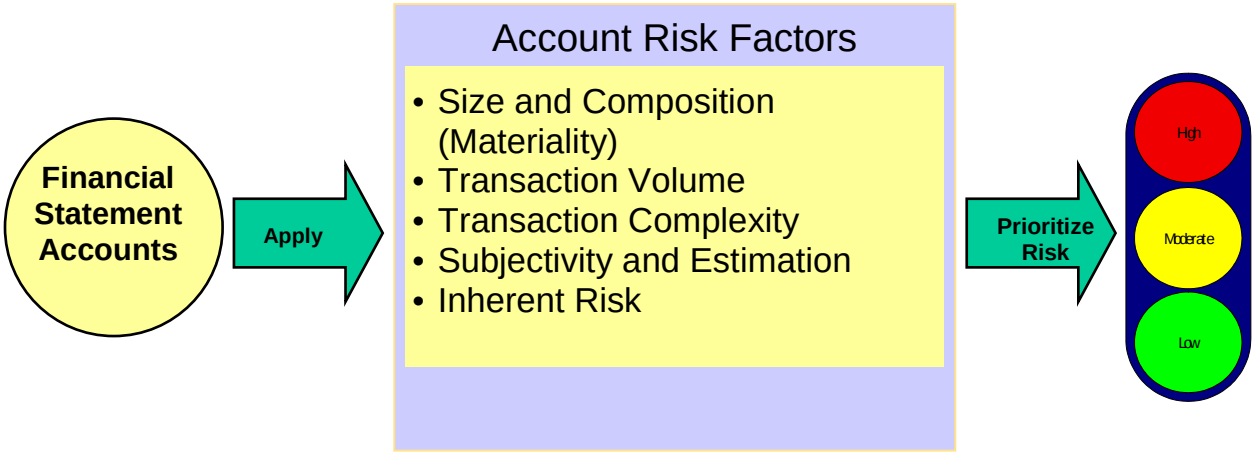
- The Financial Statement Notes and Disclosures, which provide information of the accounting policies and required footnotes to be considered in identifying financial reporting risk (if applicable)

Having worked to define the financial reporting elements, the agency will utilize the Financial Reporting Risk Assessment Criteria which considers impact and likelihood and may be used by management to prioritize the financial risks related to the financial reporting elements. The following risk factors should be considered and customized for each agency:

- Size and Composition – Criteria should be based on the agency's materiality for the associated financial statement. Refer to Appendix 4.1A for a materiality calculation and risk assessment template.

Rating	Percentage
High	≥ 5%
Moderate	5% > X > 1%
Low	≤ 1%

- Transaction Volume – Criteria should be based on the number of transactions that impact the financial element on an annual basis (e.g., number of cash receipts).
- Transaction Complexity – Criteria should be based on how routine the transactions are and/or how complex the transactions are (e.g., complex calculations, requiring significant financial statement disclosures, complex accounting guidance).
- Subjectivity and Estimation – Criteria should consider the amount of estimation that occurs within the account (e.g., determination of allowance of doubtful accounts, estimations of compensated absences).
- Inherent Risk – Criteria should be based on whether there have been audit findings (adjustments) impacting the account, whether there has been any fraudulent activity impacting the account, and/or whether there is the probability that fraud could impact the account.



The criteria above should be applied to each financial reporting element and prioritized according to risk as High, Moderate, or Low. The chart below illustrates factors which should be used when prioritizing the criteria and provides a number scale to assist in the assignment of risk.

Risk Assessment Criteria - Account

	High (Points – 3)	Moderate (Points – 2)	Low (Points – 1)
Size and Composition *Automatically populates in Risk Assessment template.*	Account balance greater than or equal to High materiality.	Account balance less than High materiality but greater than Low materiality.	Account balance less than or equal to Low materiality.
Transaction Volume *Customize for your agency per fund (## of transactions).*	Multiple transactions per day.	More than ## transactions per year but less frequent than one transaction per day.	Less than ## transactions per year.
Transaction Complexity	Transactions are complex in nature (i.e., complex calculations, requiring significant financial disclosures, complex accounting guidance associated with account, etc.).	Majority of the transactions are non-complex. However, some transactions require additional attention due to their complexity.	Transactions are routine in nature.
Subjectivity and Estimation	75% of the account balance is based on subjectivity or estimates.	Greater than 10% but less than 75% of the account balance is based on subjectivity or estimates.	Less than 10% of the account balance is based on subjectivity or estimates.
Inherent Risk *Also, includes any other risk factors not captured above.*	High probability that errors or fraud could impact the account; History of recurring or recent audit findings or material adjustments; Recent fraudulent activity.	Reasonably probable that errors or fraud could impact the account; History of past audit findings or immaterial adjustments; Past fraudulent activity.	Low probability of errors or fraud; No history of audit findings, adjustments or fraud in previous 5 fiscal years.
Total Score	Total Score of 12 or greater.	Total Score less than 12 but greater than 8.	Total Score of 8 or less.

When prioritizing risk of the criteria shown above, the following are additional example considerations in determining the overall High, Moderate or Low assessment:

- An account may be high dollar value, such as capital assets, but present low risk of material misstatement because of the nature of the transactions.
- A high-value asset or income statement account may have higher risk characteristics because there is greater chance of overstatement error.

- For liability accounts, size considerations are different from asset accounts because the risk is that the account balance will be understated.

- An account that has a small balance relative to materiality has a lower risk of financial statement error, lower level of subjectivity and estimation, and lower risk of fraud would likely result in an overall low risk prioritization.

It is important to note that the overall risk rating is judgmentally based on the aggregation of the individual risk assessments. Justification for the overall assessment should be documented.

By establishing a risk profile for financial reporting elements, the agency can more easily identify and prioritize financial reporting risks that exist in processes that affect the elements. Additionally, the amount of evidential matter needed to support the assessment increases with the associated level of risk.

NOTE: Agencies are required to perform a risk assessment for all financial statement account captions. If you can qualitatively assess risk at the statement caption level, you do not need to drill down to the account level. If not, you will need to drill down and assess risk at the account level. Of these accounts, all that meet the materiality criteria must be assessed. If some of the accounts are similar in nature, you may group them and should assess risk for the group if it meets the materiality threshold. If none of the accounts or group(s) of accounts meets the materiality criteria, then you should assess risk for the group(s) or account(s) that in your judgment are most significant to your agency.

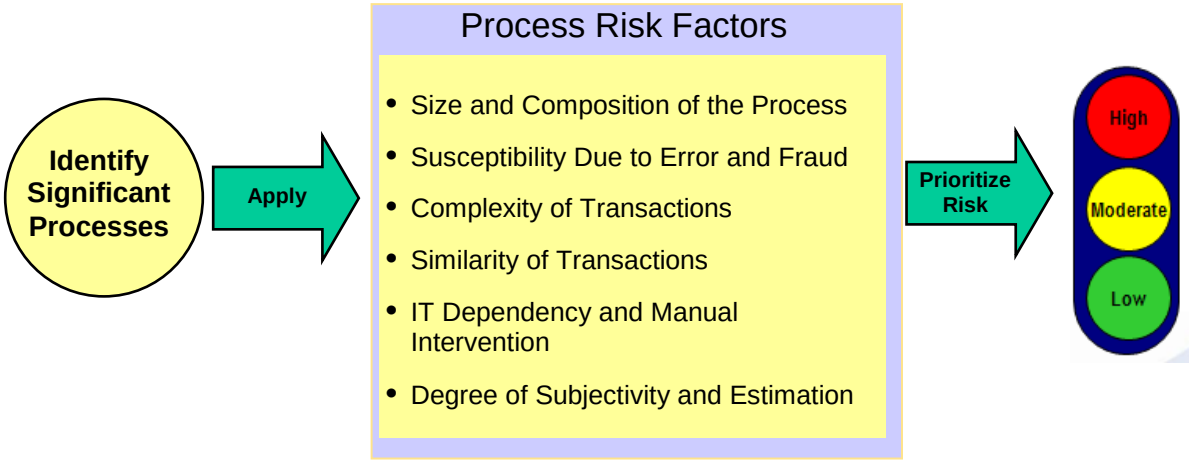
Assessing Process Risk

After using the financial reporting elements to identify account risk, attention must be turned to the individual processes that support the major classes of transactions affecting the material financial reporting elements. These may be identified through discussion with management. Major classes of transactions are those transactions that are significant to the agency's financial statements. For example, an agency may purchase goods for use in the business (e.g., office supplies), or services (i.e., contracted work). These two types of purchases would represent two major classes of transactions within the purchasing process; both significant to the agency's financial statements. Classes of transactions may be routine, non-routine or estimation (for further discussion on the types of transactions, refer to Chapter 5).

Criteria to assess risk at the process level are developed by management in a similar manner to those at the account level. By applying the criteria to each process associated with the significant accounts identified previously, agencies identify the processes that are most susceptible to material misstatement.

Each of the following Process Risk factors should be considered and customized for each agency:

- Size and Composition – Criteria should be based on the agency's materiality for the associated account. When used to determine process risk, the percentage of the account balance affected by the process needs to be considered.
- Susceptibility Due to Error or Fraud – Criteria should be based on whether there have been audit findings impacting the process, whether there has been any fraudulent activity in the process, and/or whether there is the probability that fraud could impact the process.
- Complexity of Transactions – Criteria should be based on how complex the calculations are in making the transactions and/or the complexity of the accounting standards impacting the process.
- Similarity of Transactions – Criteria should be based on how similar the calculations are in making the transactions and should consider how many locations and personnel are used in the process.
- IT Dependency and Manual Intervention – Criteria should be based on the level of automation in the process. Criteria should also consider the level of manual correction required.
- Degree of Subjectivity and Estimation – Criteria should consider the amount of estimation that occurs within the process.



Process risk criteria may be unique for each significant account. What may be considered a high dollar impact in one account may be low in another due to the size and composition of individual accounts, etc. The definitions for High, Moderate and Low are, therefore, developed to be relevant to the significant account.

The chart below illustrates factors which should be considered when prioritizing the criteria and provides a number scale to assist in the assignment of risk.

Risk Assessment Criteria - Process

	High (Points – 3)	Moderate (Points – 2)	Low (Points – 1)
Size and Composition	Process impacts the account balance by greater than or equal to 30% of account balance.	Process impacts the account balance by less than 30% but greater than 10% of account balance.	Process impacts the account balance by less than or equal to 10% of account balance.
Susceptibility Due to Error / Fraud	High probability that errors or fraud could impact the process; History of recurring or recent audit findings and/or material adjustments impacting the process; Recent fraudulent activity in the process.	Reasonably probable that errors or fraud could impact the process; History of past audit findings and/or immaterial adjustments impacting the process; Past fraudulent activity in the process.	Low probability of errors or fraud; No history of audit findings or fraud impacting the process in previous 5 fiscal years.
Complexity of Transactions	Business and accounting transactions are highly complex.	Business and accounting transactions are moderately complex.	Business and accounting transactions are not complex.
Similarity of Transactions	Less than 25% of the transactions are similar in nature.	Between 25% and 75% of the transactions are similar in nature.	At least 75% of the transactions are similar in nature.
IT Dependency / Manual Intervention	Highly manual complex processes. IT infrastructure is an older version with many manual interfaces.	Moderately automated process.	Highly automated process.
Degree of Subjectivity / Estimation	75% of the account balance impacted by the process is based on subjectivity or estimates.	Greater than 10% but less than 75% of the account balance impacted by the process is based on subjectivity or estimates.	Less than 10% of the account balance impacted by the process is based on subjectivity or estimates.
Total Score	Total Score of 15 or greater.	Total Score less than 15 but greater than 10.	Total Score of 10 or less.

Just as in assessing account risk, it is important to note that the overall process risk rating is judgmentally based on the aggregation of the individual risk assessments. Justification for the overall assessment should be documented.

Assessing Location Risk

In order to identify financial reporting risks in multi-location agencies, management needs to understand how financial reporting elements exist at the various locations and how processes at the various locations build up the balance of the related account. The purpose of this task is to assist management in identifying the locations associated with the material financial reporting elements and related processes. Assessing location risk and mapping the organization's operating locations to the significant processes enables the organization to understand where the processes are at greatest risk of failure. This can then be considered when defining the testing strategy and approach (to make certain that high risk locations are included within the testing scope).

Factors that should be considered when assessing Location Risk include (but are not limited) to the following:

- Prior Year Issues – Criteria should consider any issues that resulted in a prior year audit adjustment as well as any previous control failures.
- IT Environment – Criteria should consider the complexity of the automated processes as well as the age and vendor of the IT systems in place.
- Complexity of Business and Accounting Transactions – Criteria should take the nature of the business and accounting transactions into account.
- Changes in Business or Accounting Transactions – Criteria should be based on the number and frequency of accounting changes or significant changes to the business.
- Quantitative Significance – Criteria should be based on the agency's definition of a material impact to the consolidated financial statements.

Examples of the criteria that can be used to assess location risk are described below:

Risk Assessment Criteria - Location

	High (Points - 3)	Moderate (Points - 2)	Low (Points - 1)
Prior Year Issues	Significant prior year errors or issues resulting in audit findings and/or material adjustments or restatements. Prior year issues due to control failure.	Prior year errors or issues that did not result in audit findings and/or material adjustments or restatements. Prior year issues due to control failure.	No prior year issues.
IT Environment	Highly manual complex processes. IT infrastructure is from unknown vendor and/or version is more than 10 years old.	Moderately automated processes. Leverage some automated controls. IT infrastructure is from reputable vendor and version is between 5 and 10 years old.	Highly automated processes. Leverage automated controls. IT infrastructure is from renowned vendor and version is less than 5 year old.
Complexity of Business and Accounting Transactions	Business and accounting transactions are complex.	Business and accounting transactions are moderately complex.	Business and accounting transactions are not complex.
Changes in Business or Accounting Transactions	Rapid growth in business. Developing or offering new products/services. Significant change in the business model.	Moderate growth in business. Developing or offering some new products/services.	Maintain consistent products/services from prior years. Consistent business model.
Quantitative Significance	Account balances are significant to more than 5% of consolidated financial statements.	Account balances are significant to between 1% and 5% of consolidated financial statements.	Account balances are significant to less than 1% of consolidated financial statements.
Total Score	Total Score of 12 or greater.	Total Score less than 12 but greater than 8.	Total Score of 8 or less.

Financial Statement Assertion Risk Guidance

Within its financial statements, an organization implicitly makes claims regarding its financial position, results of operations and cash flows. Such claims are known as financial statement assertions.

Once financial reporting elements have been identified, the agency will identify the relevant financial statement assertions associated with the elements (refer to Appendix 4.2C Financial Statement Assertion Risk Guidance worksheet). This step is important because it helps the agency understand the most appropriate test objective for each financial reporting element.

An account balance can generally be misstated under three conditions: missing entries, erroneous entries, and the presence of entries that do not belong in the account. Testing an account balance

will, therefore, require verifying that the recorded transactions have occurred and belong in the account (existence or occurrence), searching for omitted items or transactions that should have been recorded in the account (completeness), considering whether the assets and liabilities belong to the agency (rights and obligations), testing whether the entries have been recorded for the correct amounts (valuation or measurement/allocation), and confirming the accounts are accurately presented (presentation and disclosure).

Financial statement assertions are presented in five categories:

- **Existence or Occurrence**
  Existence - Balance Sheet focused - Assets, Liabilities and Fund Balance exist as of the statement date.
  Safeguarding of Assets - Access to assets and critical documents that control their movement are suitably restricted to authorized personnel.
  Occurrence - Operating Statement focused - Transactions and events that have been recorded actually occurred during the accounting period and pertain to the entity.

- **Completeness**
  Completeness - All transactions and events that should have been recorded have been recorded on the Balance Sheet or Operating Statement.
  Cut-Off - Transactions and events have been recorded in the proper period.

- **Rights and Obligations** (*This assertion only applies to the Balance Sheet accounts.)*
  Rights - The entity holds the rights to the assets.
  Authorization - Transaction are executed in accordance with management's general and specific authority.
  Obligations - Liabilities recorded are the obligation of the entity.

- **Valuation or Allocation**
  Valuation - Amounts based on estimates and judgments are in accordance with U.S. GAAP.
  Allocation - Costs are allocated from the Balance Sheet to the Operating Statement in the proper period (e.g., depreciation and amortization)
  Accuracy - Amounts recorded are mathematically accurate.

- **Presentation and Disclosure**
  Presentation (Classification) - Transactions and events have been recorded in the proper accounts.
  Disclosure - Financial information is appropriately described in the financial statement notes and is understandable to users.

It is important to note that assertions are indicators of where risk could lead to financial misstatements. Prioritization of the assertions for each financial reporting element assists in determining the need for controls to mitigate risks related to the assertions. If the risk of an assertion to an account is high, a more rigorous set of direct transaction and/or monitoring controls would be needed to satisfy the assertion.

Evaluating the Results

After assessing risk at the account, process and location levels, the results may be tallied to produce a preliminary risk profile by account (refer to Appendix 4.1A for a risk assessment template). As the risk level increases, the level of testing effort required to achieve sufficient reliance over the control environment also increases.

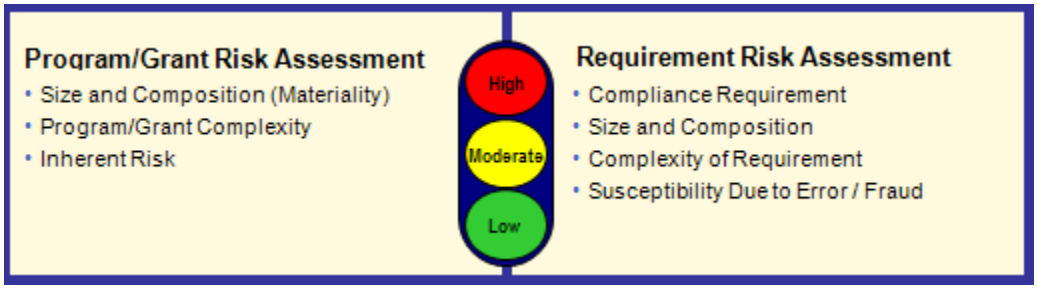
Fully understanding the key processes covering major classes of transactions that ultimately support the material financial reporting elements is a critical aspect of management's ability to identify financial reporting risks. Therefore, management is required to document their significant processes to support their annual risk assessment.

For an in-depth review of process documentation, refer to Chapter 6.

Compliance Risk Assessment

The compliance risk assessment is based around the two risk components previously introduced. Criteria are developed for each component, and are based around risk factors that can be tailored by the organization. Information to develop the risk assessment criteria is obtained from a number of sources to understand the organizational structure, strategy, management, fraud prevention and operational issues faced by the organization. Each criterion is developed with key stakeholders and is then validated with senior personnel.

Components of the Compliance Risk Assessment



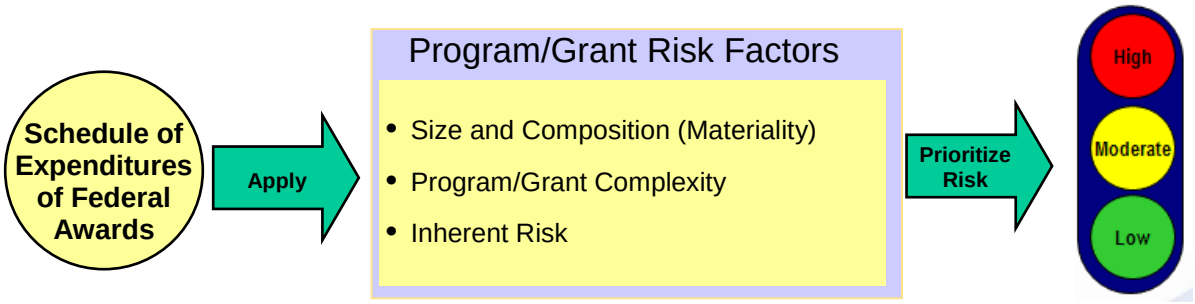
Assessing Program/Grant Risk

In performing the risk assessment, the agency will first obtain the Schedule of Expenditures of Federal Awards (SEFA) report (FED-11) and assess the risk for each of the program/grants for the following factors:

- Size and Composition – Criteria should be based on the agency's materiality for the associated program/grants disbursements. Refer to Appendix 4.1B for materiality calculation and risk assessment template.

Rating	Percentage
High	≥ 50%
Moderate	10%> <50%
Low	≤ 10%

- Program/Grant Complexity – Criteria should be based on how routine the program/grants are and/or how complex the program/grants are (i.e., the experience/knowledgeable staff; changes to or any new compliance requirements).
- Inherent Risk – Criteria should be based on whether there have been audit findings impacting the program, whether there has been any fraudulent activity impacting the program, and/or whether there is the probability that fraud would impact the program.



The criteria above should be applied to each Program/Grant element and prioritized according to risk as High, Moderate, or Low. The chart below illustrates factors which should be used when prioritizing the criteria and provides a number scale to assist in the assignment of risk.

Risk Assessment Criteria - Materiality and Program/Grant

	High (Points – 3)	Moderate (Points – 2)	Low (Points – 1)
Size and Composition *Automatically populates in Risk Assessment template.*	Program/grant expenditures greater than or equal to High materiality.	Program/grant expenditures less than High materiality but greater than Low materiality.	Program/grant disbursements less than or equal to Low materiality.
Program/Grant Complexity	New or complex program/compliance requirements; Less experienced or new compliance personnel.	Majority of the program/compliance requirements are non-complex. However, some requirements involve additional attention due to their complexity.	Non-complex compliance requirements. Highly experienced and knowledgeable compliance personnel.
Inherent Risk *Also, includes any other risk factors not captured above.*	High probability that errors or fraud could occur; History of recurring or recent audit findings or recent fraudulent activity.	Reasonably probable that errors or fraud could occur; History of past audit findings or past fraudulent activity.	Low probability of errors or fraud; No history of audit findings or fraud in previous 5 fiscal years.
Total Score	Total Score of 7 or greater.	Total Score of less than 7 but greater than 4.	Total Score of 4 or less.

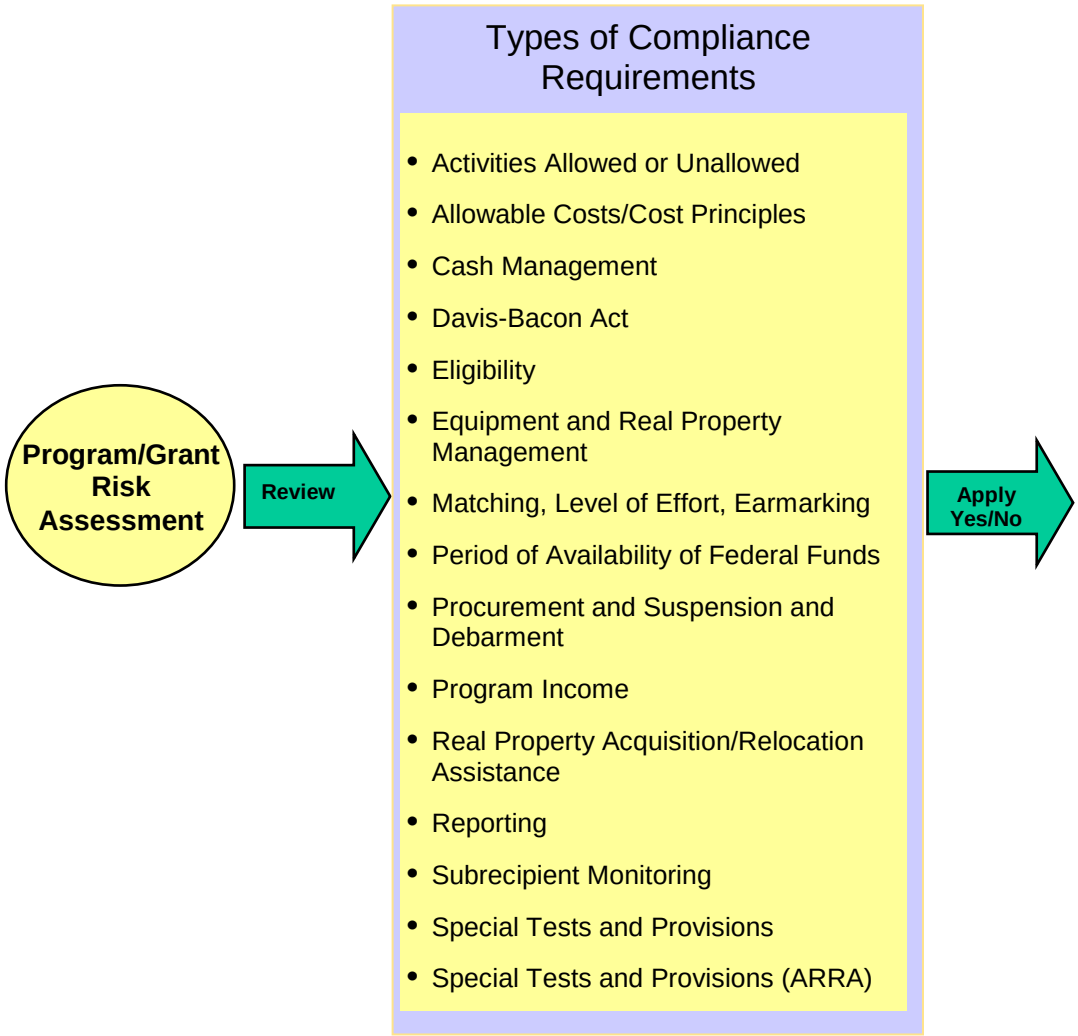
It is important to note that the overall risk rating is judgmentally based on the aggregation of individual risk assessments. Justification for the overall assessment should be documented.

Note: Agencies are required to perform a risk assessment for all program/grants listed on the Schedule of Expenditures of Federal Awards. The SEFA schedule is the prior year's expenditures thus, if you are aware of new programs/grants that will begin during the current year, you should add them to the risk assessment and rate the new program/grant based on the budgeted expenses.

Assessing Requirement Risk

After using the Schedule of Expenditures of Federal Awards to identify the program/grant risk, attention must be turned to the individual requirement risk that supports each program/grant. These may be identified by review of the A-133 tab on template 01 (Appendix 4.1B), review of grant agreements, and review of Circular A-133 (www.whitehouse.gov).

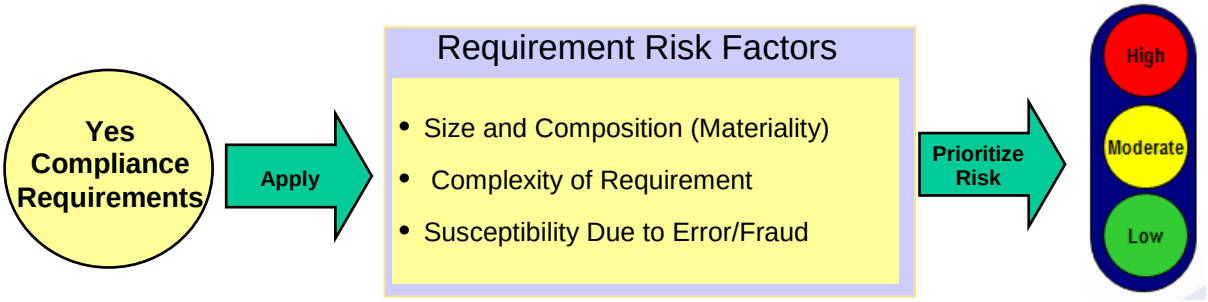
To assess risk for the individual compliance requirement, an agency must first determine whether the requirement is applicable. If the requirement is applicable, you will select "yes" in the drop down menu and "no" if it is not applicable. The A-133 tab will assist in determining whether the requirement is applicable by each Catalog of Federal Domestic Assistance (CFDA) number and compliance requirement. If the compliance requirement does not apply, no further work is necessary for that requirement. If the requirement is applicable, you will need to risk rate the requirements.



Criteria to assess the requirements are similar to those at the program/grant level. By applying the criteria to each requirement, agencies identify the requirements that are most susceptible to noncompliance.

Each of the following requirement risk factors should be considered for each applicable compliance requirement:

- Size and Composition – Criteria should be based on the agency's materiality for the associated program/grant. For example, if Reporting is an applicable compliance requirement, it applies to 100% of the population (total expenditures), thus this would be a high rating for size and composition.
- Complexity of Requirement – Criteria should be based on the complexity of the program/grant requirement.
- Susceptibility Due to Error/Fraud – Criteria should be based on whether there have been audit findings impacting the requirement, whether there has been any fraudulent activity affecting the requirement, and/or whether there is the probability that fraud could impact the requirement.



The chart below illustrates factors, which should be considered when prioritizing the criteria and provides a number scale to assist in the assignment of risk.

Risk Assessment Criteria - Requirement Risk Factors

	High (Points – 3)	Moderate (Points – 2)	Low (Points – 1)
Size and Composition	30% or more of grant expenditures are applicable to this compliance requirement.	Greater than 10% but less than 30% of grant expenditures are applicable to this compliance requirement.	Less than 10% of grant expenditures are applicable to this compliance requirement.
Complexity of Requirement	Compliance requirement is new and/or highly complex.	Compliance requirement is non-complex. However, some aspects of the requirement involve additional attention due to the complexity.	Compliance requirement is not complex.
Susceptibility Due to Error / Fraud	High probability that errors or fraud could occur; History of recurring or recent audit findings or recent fraudulent activity.	Reasonably probable that errors or fraud could occur; History of past audit findings or past fraudulent activity.	Low probability of errors or fraud; No history of audit findings or fraud in previous 5 fiscal years.
Total Score	Total Score of 7 or greater.	Total Score of 6.	Total Score of 5 or less.

Just as in assessing program/grant risk, it is important to note that the overall requirement risk rating is judgmentally based on the aggregation of the individual risk assessments. Justification for the overall assessment should be documented.

4.3 IMPACT ON INFORMATION TECHNOLOGY

Application scoping is an output of the risk assessment process. Properly scoping applications requires an understanding of the critical IT functionality relied upon to facilitate the proper operation of business processes. During the identification of risk, management seeks to identify those applications impacting and affecting the significant processes identified in the risk assessment.

Identifying Significant Applications

Financially significant applications are those with critical IT functionality or data (see definitions below) to significant processes as identified by the risk assessment. Applications that are involved in the processing of financial transactions but neither contain critical IT functionality nor data that is subject to unauthorized change (that could lead to a material error) are not considered significant applications.

Financially significant **applications** are relied upon during the financial reporting process, including significant automated application controls, significant reports and other significant automated processes. If an application does not operate consistently and correctly, there is at least a reasonable likelihood of an error that would not be prevented or detected. To be included, the functionality has to be necessary to detect or prevent transaction errors (i.e., part of a control).

Data is financially significant when, affected by an unauthorized change that bypasses normal application controls (for example, as a result of an IT General Controls failure), it is at least reasonably likely that a financial statement error that would not be prevented or detected will occur.

For applications that are not considered financially significant based on the presence of critical IT functionality, it is management's responsibility to assess whether an unauthorized change directly to the application's data could result in an undetected financial statement error. This step determines whether a change to the data, bypassing the normal process and controls (sometimes referred to as "backdoor access"), could result in a material error in the financial statements that would not be detected by the normal operation of controls. If this is the case, the application should be assessed as a financially significant application. If not, the application may be considered out of scope for assessment purposes.

On occasion, calculations and other functionalities use data created in a prior application. Where a change to that data could result in an undetected material error, the risk may reside not only within the application that uses the data but also in other applications (for example, the application where the data was created and any other applications where the data was stored). If changes to the data in those applications could go un-detected, each of these upstream applications may be financially significant.

As management completes the risk assessment process, one of the key outputs of this process is the initial application scoping. Only financially significant applications are included within this scope; however, as management begins to document process and controls in later steps, additional information may be learned which would require the addition or deletion of one of the initially scoped applications. Therefore, management should consider application scoping throughout the process, while initially focusing on those applications defined as part of the risk assessment process.

5. INTRODUCTION TO PROCESSES AND CONTROLS

5.1 INTRODUCTION

A strong understanding of processes and controls is necessary when conducting an internal control assessment, including an awareness of the compliance requirements. This chapter is devoted to identifying the types of processes, including compliance requirements, and their components, identifying the types and nature of controls, and describing basic IT process and control concepts. The different types of processes include executive processes, operating processes, and support processes; and the process components consist of process boundaries, process inputs, process activities, and process outputs. Controls may be prevent or detect, and there are three main types of controls - manual, IT-dependent manual, and IT application. IT general controls protect the systems that support the relevant processes and allow for reliance on IT application and IT-dependent manual controls. Additionally, end-user computing controls should be a consideration when conducting an internal control assessment.

5.2 UNDERSTANDING PROCESSES

Processes Defined

A **process** is a group of logically related activities that, when performed, use the resources of an organization to produce definitive results or transform input through a series of activities into a product or service. More simply stated, a process is a group of logically related activities that transform inputs into outputs.

Significant processes are major processes where significant classes of transactions are initiated, recorded, processed and/or reported (e.g., financial close process). Within processes, one may identify a variety of types or classes of transactions.

Classes of transactions are data, information, or account detail of a common nature within the financial or other processes of a business (e.g., sales, purchase of goods or services, recording depreciation expense). A transaction is generally considered to be of a separate class if its processing differs from other classes of transactions in any significant respect and, therefore, is susceptible to different inherent and/or control risks. (Risks are discussed in greater detail in Chapter 4.)

Compliance requirements are based on OMB Circular A-133 which is applicable to federal programs/grants. Management may find it helpful to review the relevance of each compliance requirement within the Compliance Internal Controls Guidance (Appendix 4.2D) related to each program/grant.

Transaction types can be distinguished if they are processed differently during part or all of their flow through the system and, in particular, if they are subject to different controls. If different transaction types are *not* properly distinguished, later testing of internal controls

may be based on incorrect assumptions about the underlying population of items and may produce misleading results.

Transactions are classified by the following types:

- **Routine transactions** are recurring activities performed in the normal course of business (e.g., payroll, invoicing and recording to the general ledger).

- **Non-routine transactions** are activities that occur periodically that are not part of the routine flow of transactions (e.g., accrual entries).

- **Estimation transactions** are activities that involve management assumptions (e.g., allowance for bad debt).

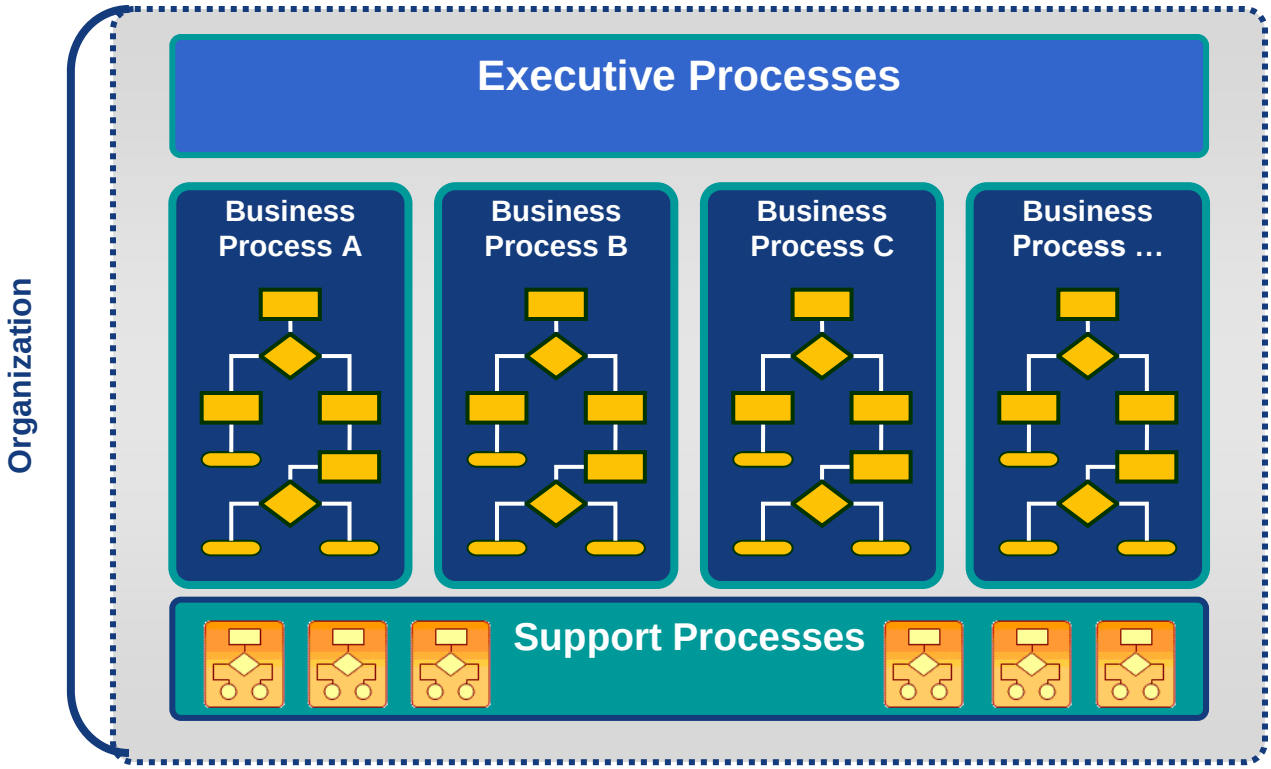
Both non-routine and estimation transactions are considered "13th month" transactions for the State of North Carolina.

Attention should be focused on significant transaction types. In many cases, similar transaction types can be documented together, either in a single set of flowcharts, which include explanatory notes for any important differences, or the same process narrative.

Process Types

In every organization there are three types of processes: executive, operating and support. **Executive processes** define and monitor the strategy and activities necessary to achieve the defined objectives of an organization, such as strategic planning or corporate governance. **Operating processes** are those processes that drive an organization's core business, such as sales or services. **Support processes** are non-core business processes necessary to operate an organization. Examples of support processes include corporate accounting, payroll and human resources.

Depending on the organization, some processes may be classified as operating or support. For example, at a manufacturing organization, purchasing is an operating process as it is core to manufacturing operations, while at a university, purchasing is a support process as it does not relate to the university's core business.



Process Components

Process boundaries include the logical beginning and ending of a process. These may be different for different organizations. It is important to understand process boundaries as they impact the scope of review. Boundaries determine what is included in the process as well as what is excluded. Boundaries define sources of inputs to the process and the destination of outputs from the process. An agency's review of a process may not always examine the entire process from beginning to end, or alternatively, may extend beyond the process boundaries.

One should be aware of the scope of the process in question, which should provide details relating to the point in the process where the review begins. For example, an organization may need to document a payroll process, with the exception of the new hire set-up process, which is performed by another organization. As a result the process documentation might begin with the time entry process for hourly employees.

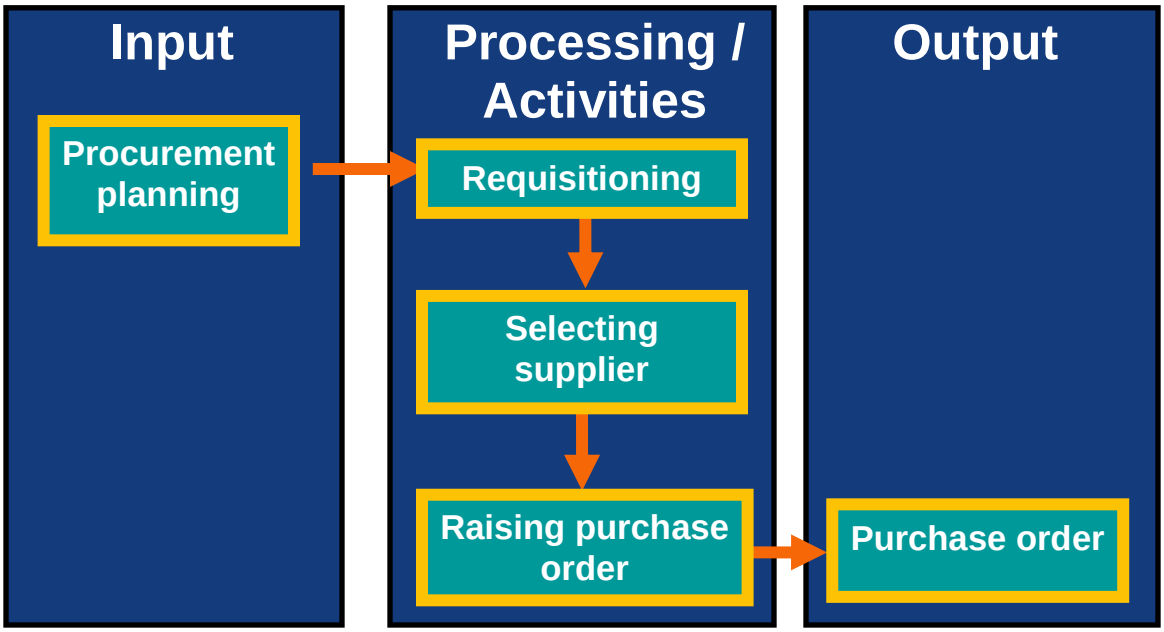
A process has three main components: inputs, activities and outputs. It is important to understand the difference between the different components. They can be defined as follows:

Process Inputs are the material, capital, human resources and information that a business process receives and acts upon in order to transform it into its output.

A **Process Activity** is a specific deed, action or function designed on its own or with other related activities to turn input into output.

Process Outputs are those things transformed by a process for the benefit of the customer or for use as an input in a later process or activity.

The following diagram depicts example process inputs, activities and outputs for a purchasing process:



5.3 UNDERSTANDING CONTROLS

Internal Controls

The North Carolina General Assembly's House Bill 1551 defines **internal control** as an integral process, affected by an entity's governing body, management, and other personnel, designed to provide reasonable assurance regarding the reliability of financial reporting, compliance with applicable laws and regulations, and achievement of objectives related to the effectiveness and efficiency of operations.

Internal controls may be either prevent or detect. Both are important to the analysis of a process and may exist together within the same process.

Prevent controls, as the name implies, are those used to prevent errors from occurring (i.e., to prevent the wrong source documents from being entered into the system or to prevent an irregularity from taking place). Examples include use of approval matrices, automated validity and edit checks, sequential pre-numbering of checks and logical access security.

Detect controls are those used to detect any error or irregularity after it has occurred. These include independent checking and review, exception monitoring routines and reconciliations.

Prevent controls are usually easy to identify, since they generally operate on every transaction of a given type and are often automated. Where effective prevent controls exist, the likelihood of errors is low and the need for extensive detect controls reduced.

Conversely, where prevent controls are not sufficient, there is a greater need for particularly sensitive and effective detect controls. Detect controls are less likely to be applied to every transaction during the normal flow of processing and may only be performed at intervals. They are also less likely to be fully automated, may be less formalized and may be more difficult to identify.

Good detect controls can sometimes compensate for the absence of adequate prevent controls. Even if informal, controls can be effective if they capture all relevant data completely and accurately, identify all potentially significant errors, are performed on a consistent and regular basis and include timely follow-up of errors and problems detected. Consequently, care must be taken to understand all of the relevant controls before developing conclusions and recommendations on the control system.

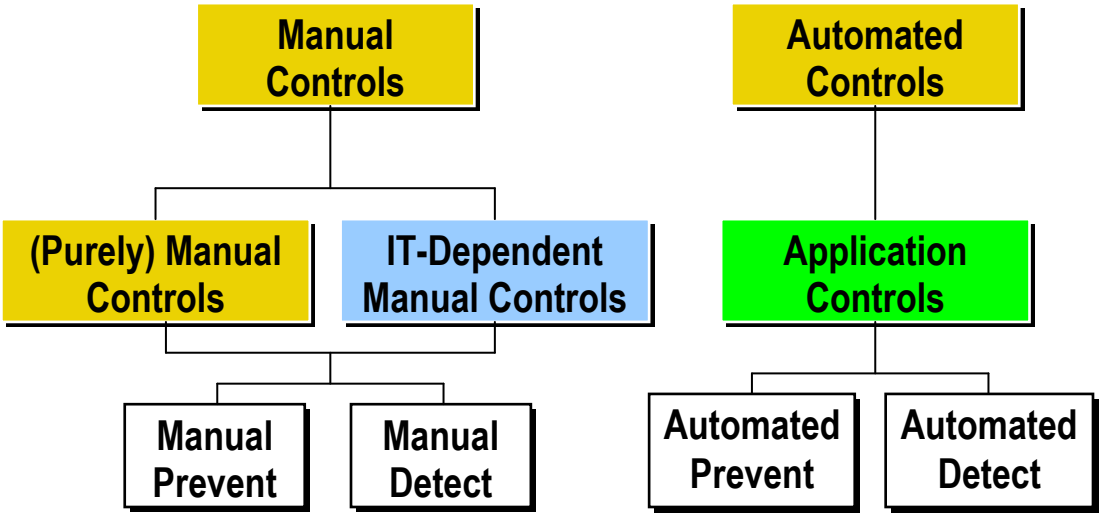
Nature of Controls

At the transaction level there are three types of controls:

Manual controls, as the name implies, are those controls that are manually performed by an individual. Examples include the independent review of general ledger reconciliations or the authorization of employee expense reports.

IT-dependent manual controls are those controls that are manually performed, but require input based upon the results of computer-produced information. Examples of IT-dependent manual controls include management's review of a monthly variance report and follow up with significant variances. Management relies on the computer-produced report to identify and generate variances.

IT application controls are performed entirely by a computer or computer-based system. Examples of IT application controls include an automated three-way match, data input validation checks and restricted user access.



It is important to understand the nature of a control in order to properly design effective testing methods to determine if the control is designed and operating effectively. (For more information on Testing Theory and Strategy, refer to Chapter 7.)

Frequency of Controls

It is important to understand the frequency at which a control is performed, as this helps in determining the design effectiveness of a control as well as what sample size is appropriate for testing the operation of the control. (Sample sizes are discussed further in Chapter 7.)

Controls may be performed at any one of the following frequencies:

Frequency	**Example**
Continuous	Firewall
Daily / Multiple times per day	Three-way Match
Weekly	Weekly timesheet review and approval
Monthly	Review of general ledger reconciliations
Quarterly	Review of access to IT systems
Annually	Review of accounting policies
Ad hoc / As required	Authorization of termination payment to employee

Control Owner

Understanding who owns the control assists in the determination of effective control design. For example, general ledger reconciliations are performed by the accountant rather than the goods receiving clerk. It is also important to understand who is responsible for the custody, authorization and recording of transactions in order to determine if appropriate segregation of

duties exists. Finally, identifying the control owner identifies whom to contact to understand and test the control.

How to Write a Control

When writing a control, it is important to document the following:

1. Who performs the control activity?
2. What is the control activity (not the process)?
3. When is the control activity performed?
4. How is the control activity documented?

A good control description clarifies how a control is to be tested. The following control description answers each of the four questions posed above:

"Before processing each invoice (3), the Accounts Payable supervisor (1) reconciles the quantity on the goods receipt to the quantity on the invoice (2). Any discrepancies are followed up with the receiving personnel in the warehouse and documented on the invoice (4). The Accounts Payable supervisor also reconciles the quantity and price on the approved purchase order to the invoice (2). If there are differences, the Accounts Payable supervisor further investigates and resolves with the assistance of the procurement department (2)."

Determining Significant/Critical Controls

Even when controls, taken as a whole, are likely to be effective, the contribution of individual controls to that result is likely to be unequal. When using process flowcharts and a Risk and Control Matrix (discussed in Chapter 6), one should carefully consider the role that each control plays in the control system. Judgment needs to be used to determine which individual controls to consider as significant in preventing or detecting each type of error (i.e., each statement or question of "what could go wrong").

Controls should be identified as critical if they contribute to the evaluation of overall control effectiveness in precluding errors and achieving control objectives. A critical control is a control that will prevent or detect an error in the event that all other controls fail.

Identifying Redundant or Inefficient Controls

Throughout the evaluation of the control system, it is important to be conscious of the cost and inefficiency of unnecessary controls. When individual controls do not contribute materially to the overall control system, are redundant with other existing controls, or could be productively replaced by a more efficient control, management should reconsider testing or evaluating these controls.

NOTE: Although not all controls will be tested, this does not diminish or remove the need for sound internal controls throughout an agency. Controls not tested should continue to be performed to contribute to the overall control environment of an agency.

5.4 UNDERSTANDING IT CONTROL CONCEPTS

When evaluating how well risk is managed within a process or compliance requirement, it is important to understand the IT environment and IT controls that may be relied upon in order to develop appropriate test plans. Virtually all processes use IT systems; with that in mind, consider the IT environment an "umbrella" over an agency's infrastructure. If the IT environment acts as the "umbrella" over an agency's infrastructure, the agency needs controls in place to mitigate the risk of information being processed incorrectly and the risk of unauthorized access.

The relationship between processes or compliance requirements and transactions and the computer applications that support them is often complex. Processes or compliance requirements are frequently dependent on more than one computer application. In order to avoid duplication of effort in gaining an understanding of these systems, one should limit attention to those applications which are significant to the processes under review. (Refer to Chapter 6 for further discussion of IT processes which may not be under the control of an agency.)

An **application** is a software program that supports the processing of transactions and maintenance of an organization's records on electronic media. An application typically consists of programmed procedures, files and databases. A **database** is a repository for storing data in a format that can be accessed by applications for calculations and reporting. Most databases are considered pertinent to financial statement reporting because they are the location where financial data resides and could potentially be manipulated.

In order to properly restrict applications, agencies should consider the importance of IT controls. IT controls can be generally categorized as application controls, IT-dependent manual controls, End-User computing controls and IT general controls.

Application Controls

Application controls are automated controls that apply to the processing of individual transactions to provide reasonable assurance that all transactions are valid, properly authorized and recorded, and are processed completely, accurately and on a timely basis. This includes controls such as edit checks, validations, calculations, interfaces and reporting.

The following components of application controls should be considered:

- Configuration settings and custom automated controls
- Master data controls and access
- Control overrides
- Segregation of duties and function access
- Interface control

IT-dependent manual controls are specific process controls that are manually performed, but require input based upon the results of computer-produced information. Typical

IT-dependent manual controls are computer generated reports that are used to either input key financial information, or review for exception reporting.

Some examples of IT-dependent manual controls are:

- Review and follow up of exceptions on a payroll exception report.
- Review and follow up of exceptions on a customer billing cycle report.
- Hourly time summary report is manually entered into payroll system.

End-User Computing Controls

End-User Computing introduces a different level of risk to an organization's information technology and operational environment. End-User Computing generally involves the use of department-developed spreadsheets and databases, which are frequently used as tools in performing daily work. To the extent these spreadsheets are in place, they are an extension of the IT environment, and results generated from them may, in assessing their impact, have an effect on the organization's financial statements.

End-User Computing can be monitored and controlled by manual processes; using automated tools; or by the ideal method of eliminating the need for End-User Computing, i.e., by adding the computations to systems controlled by information technology.

End-User Computing monitoring typically includes:

- Identifying any and all spreadsheets and/or databases that are in use and form the basis for reports, data used in performing duties, or assist in creating financial data and transactions.
- Locating the spreadsheet and/or database on the network, including the drive and server location; or if on a desktop, locating the personnel who use the spreadsheet in conducting their duties.
- Determining personnel with access to the spreadsheet or database and identifying controls in place (i.e., version control, change control, password access, etc.) and computer security in place for these files.

In order to mitigate the risk introduced by End-User Computing, it is pertinent to confirm adequate controls are in place for those high risk spreadsheets, databases and other user-developed programs as they are equivalent to any other system. These controls should allow for processing integrity, and validate the tool's ability to sort, summarize and report accurately. Some examples of End-User controls are as follows:

- Access control - Controls that limit access to specific rights within a particular system object, such as a file directory or individual file. The most common access control is to restrict the ability to write, delete or execute a file or directory.
- Version or Change control - Controls or techniques, especially in an automated environment, to control access to and modification of documents and to track versions of a document when it is revised.

- Review for completeness, accuracy and processing integrity - Controls that confirm the data housed via spreadsheets or databases are complete and accurate.
- Backup - A control that makes copies of data so that these additional copies may be used to restore the original after a data loss event. The greater the importance of the data that is stored on the computer, the greater the necessity for data backup procedures.

Note: Spreadsheets are equivalent to any other system; therefore, it is pertinent to confirm adequate controls are in place around those 'key' or high risk spreadsheets (i.e., password protection, version control, etc.).

Refer to Appendix 5.1 for an illustrative list of End-User Computing controls to provide guidance in identifying typical controls in an agency. These lists are not all-inclusive; each assessment team will need to consider the unique End-User Computing environment of its agency.

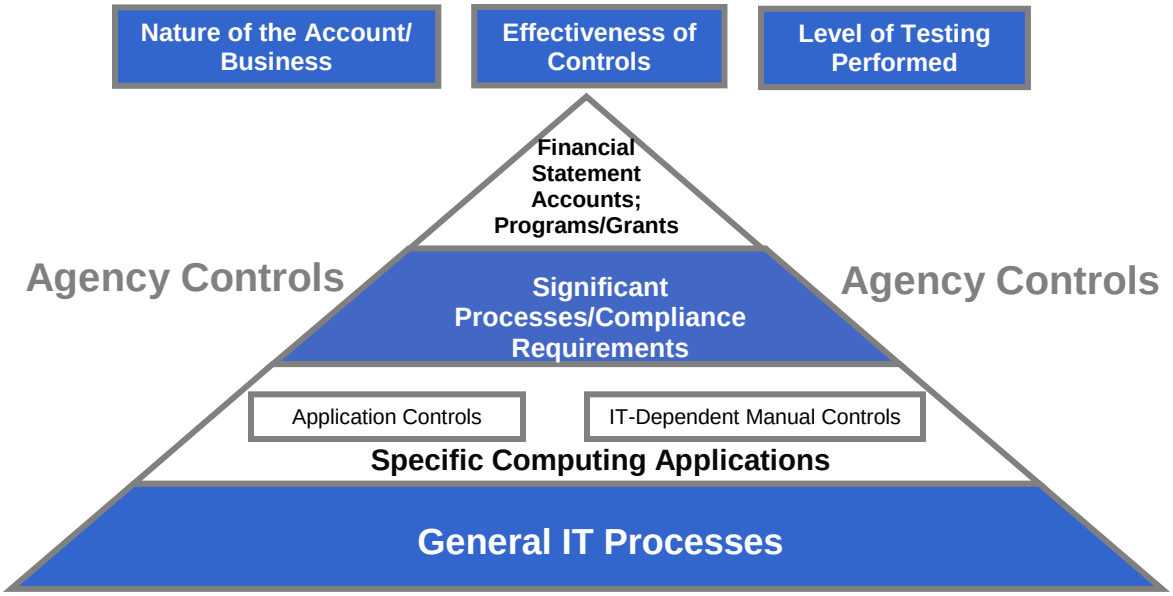
IT General Controls

IT general controls confirm that all changes to the supporting application(s) are properly requested, authorized, tested and approved before being implemented into production. This includes:

- Change Management
  - Changes are authorized, tested and approved to confirm application controls operate effectively through the period of intended reliance.
  - Changes are monitored on a regular basis for unauthorized changes.

- Logical Access
  - Access to key systems and files is approved, appropriate and monitored to confirm data generated by the applications is reliable.
  - Application Security: Higher-level logins and parameter change restrictions confirm applications are secure.

- Computer Operations
  - Data supporting the key financial information is backed-up, such that data can be accurately and completely recovered if there is a system outage or data integrity issue.
  - Programs are executed as planned, with deviations from scheduled processing being identified and investigated, including controls over job scheduling, processing, and error monitoring.



To review, business processes are supported by applications; for example, procure to pay – purchasing application, accounts payable application, inventory application, etc. The applications reside on a database (for example, Oracle DB) which houses the data, and the database resides on an operating system (platform) which is on a network which sits on a physical box in a data center.

IT general controls support reliance on IT application controls and IT-dependent manual controls within business processes. When performing control testing, agencies should also test the database, operating system and network (at the general controls level) to a sufficient extent to conclude that the overall control environment effectively mitigates risk. For further discussion of Control Testing, refer to Chapter 7.

Refer to Appendix 5.1 for an illustrative list of IT general controls considered relevant to support financial reporting and compliance objectives. This list is not all-inclusive, and each assessment team will need to consider the unique IT environment of its agency.

6. DOCUMENTATION OF PROCESSES AND CONTROLS

6.1 INTRODUCTION

Process Documentation

Process documentation can begin after holding discussions with process owners and completing the risk assessment. The results of the risk assessment will identify those specific processes or compliance requirements that require further documentation. It is important to understand the reasons for documenting a particular process or compliance requirement before beginning the documentation. Reasons to document a process or compliance requirement include the following:

- To evidence an understanding of the process or compliance requirement.
- To identify key risks and controls. Understanding the process owner's processes or compliance requirements, risks and controls is integral to meeting the objectives of the EAGLE Program.
- To identify control gaps and process improvement opportunities. The process owner will benefit from improvement opportunities that are identified through documentation.
- To facilitate the preparation of the Risk and Control Matrix and Test Plans. The Risk and Control Matrix helps to document the identified risks and corresponding controls, as well as the assessment of risk, testing strategy and results.

6.2 GATHERING INFORMATION

In order to begin documentation, one must first gather all available background information. This information may be obtained in the form of existing documentation, policies and procedures or interviews. Existing documentation often provides a starting point from which to begin. It allows the reader to gain a precursory understanding of the process and identify areas where more information is required. If existing documentation does not exist, often policies and procedures will be of some assistance.

A policy details the principles that guide the actions and decisions in an organization. Policies do not tell "how" to do something, but specify what is acceptable, unacceptable, right and wrong. An organization usually has policies addressing each of its functional areas. A compilation of these policies is a policy manual. The manual might contain the policies of the entire organization, or separate manuals may house policies for each functional department.

Procedures (also known as Standard Operating Procedures [SOPs]) address "how things are to be done." Procedures define the steps to be taken in various business situations that are typical to the organization. An organization may have the same processes established at various locations. Procedures help bring uniformity (standardization) in action across the organization.

Interviews

After reviewing existing documentation and policies and procedures in order to gain a basic understanding of a process or compliance requirement, it is recommended that interviews be conducted to capture and retain the specific details of a current process or compliance requirement. Interviews are conducted with process owners in order to inform them of the scope and approach of the assessment, obtain the process owner's preliminary assessment of key risks and controls and to understand planned changes (if any) to processes and controls. A good interview will result in an understanding of the process and compliance requirement and transaction flow as well as validate any additional information gathered prior to the interview.

When conducting an interview, consider the following:

- What are the specific activities within the process or compliance requirement?
- What are the key inputs (beginning) and outputs (ending) of the process or compliance requirement?
- What types of controls are included in the process or compliance requirement, i.e., Automated vs. Manual, Detect vs. Prevent?
- What are the decision points and alternative paths? It is important for the assessment team to identify all decision points within a process or compliance requirement, as there may be alternative paths that transactions can take. If all the alternative paths are not identified, it may not be possible to identify all of the key risks and controls.
- What are the integration points with other areas of the organization? Because risks are present at integration points with other areas of the organization, it is important to understand where these integration points are. If required, identify contacts for additional information.
- What are the key IT systems supporting the process or compliance requirement? The supporting IT systems may determine how transactions are processed and recorded, as well as the types of risks and controls included.
- Who are the responsible personnel within a process? Identify positions. Names are not sufficient, because there may be changes over time.
- What is the time frame of the process or compliance requirement? It is important to understand both the actual and elapsed time for tasks in the process.
- What is the impact on the financial statements? What general ledger accounts are affected?
- What are the key performance measures, monitoring controls and reporting controls?
- What are the Process or Compliance Owner's key concerns (risk areas)?
- Is there a history of problems with key controls or process areas?
- Are there any potential compensating controls within the process?
- What is the impact of control breakdowns (if known)?

A successful interview will answer these types of questions. If all of the questions cannot be answered in one interview, it is possible to request and complete a follow-up interview.

6.3 DOCUMENTING AN UNDERSTANDING OF PROCESSES

After the interview has been completed, it is important to record an understanding of the transaction flow for significant processes or compliance requirements and transaction types. This may be accomplished through a flowchart, process narrative, or both. A **flowchart** is a diagram that shows the step-by-step progression through a procedure or system using connecting lines and a set of conventional symbols. Flowcharts provide a concise, efficient means of depicting the sequential flow of documents and information, the interaction with key files, and the relevant processing procedures and control points. When properly done, they are easy to read, understand and update. (Refer to Appendix 6.3 for a flowchart example.)

Narrative descriptions of the transaction flow may be used as a supplement to flowcharts or as stand-alone documentation. In general, the assessment team should choose the form of documentation that is most efficient and effective for the current assessment, without losing sight of the longer-term benefits of creating automated flowcharts that can be updated quickly on future occasions. (Refer to Appendix 6.1A & Appendix 6.1B for narratives.)

The process or compliance requirement documentation should reflect all the relevant processing procedures, whether manual or automated. Integration of both manual and computerized processes is essential to gaining a complete understanding of the control system. When complex or unusual systems are involved, an individual familiar with these systems should take a lead role in providing and recording the understanding of key procedures and in working directly with supporting technology management, if appropriate. The results of this work should be fully integrated into a single set of documentation.

For each significant class of transactions, the documentation (flowchart and/or narrative) should reflect, to the extent practicable, all the relevant procedures, whether performed manually or automated.

Routine transactions

- Major input sources
- Important data files, documents, and records
- Significant processing procedures, including online entry and updating processes
- Important output files, reports, and records
- Functional segregation of duties

Non-routine transactions

- The procedures or forms used
- Any computer applications or databases/files used in the accounting activities
- The assumptions, if any, employed in the transaction
- The frequency with which the non-routine transaction occurs
- The personnel involved

Estimation transactions

- The data used to make the estimate
- The relevant factors and assumptions used to make the estimate
- The techniques used to apply the assumptions to the data, including the procedures to collect, calculate, and aggregate the relevant data
- The frequency with which the estimation transaction occurs
- The degree of subjectivity involved
- The personnel involved in making the estimate

When documenting a process or compliance requirement, risks and controls should be the major focus. The documentation should provide evidence that appropriate controls have been established and are effectively designed to prevent or detect errors of importance or fraud. The documentation should include a description of the control, including how the control is performed, who performs the control, what data reports, files, or other materials are used in performing the control and what physical evidence, if any, is produced as a result of performing the control. This documentation will be helpful in subsequent phases of the assessment process, particularly in designing testing procedures to verify the operating effectiveness of those controls. Controls should be referenced within the process or compliance requirement documentation (numbered reference) to allow for easy identification in subsequent assessment steps.

Generally, documentation of the controls over significant applications and transactions is sufficient when it:

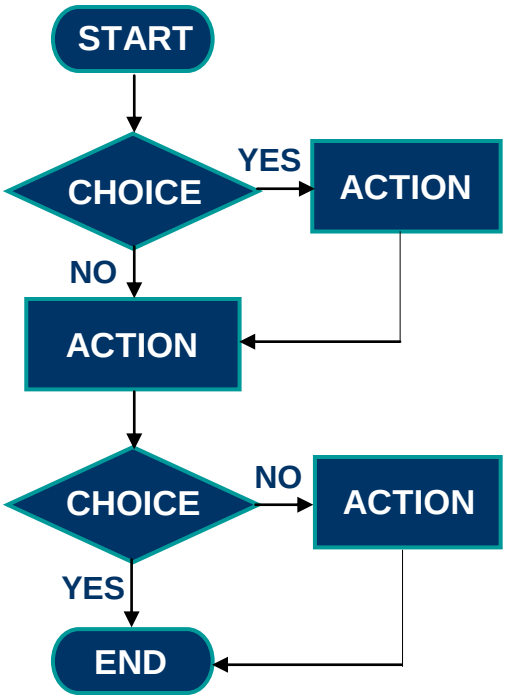
- Specifies "what could go wrong" in the processing stream and thus where controls are needed
- Describes the relevant prevent and detect controls that are responsive to each "what could go wrong" question
- States who performs the controls and how frequently

Flowcharts

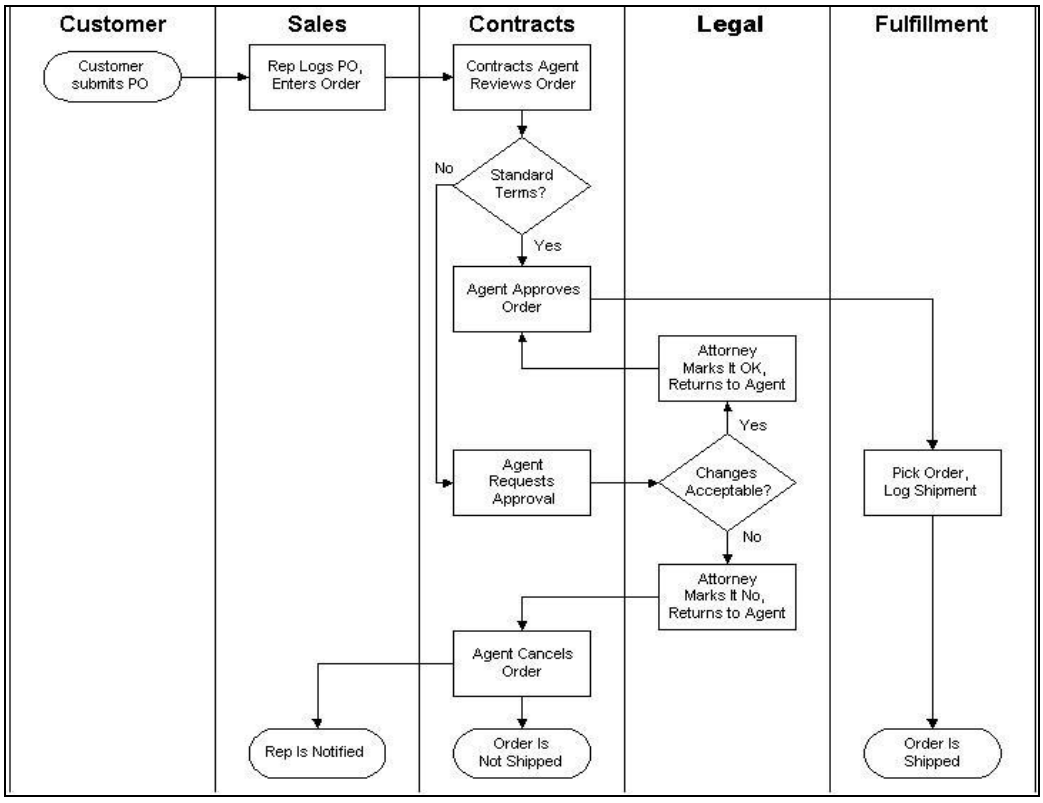
Flowcharts are utilized to break down processes into individual events and activities which help identify interdependencies across the organization by linking system and manual activities. Additionally, the flowchart helps identify gaps, weaknesses, segregation of duties problems and potential inefficiencies in a process.

Types of Flowcharts

- **Linear Flowchart -** A diagram that displays the sequence of work steps that make up a process. This tool can help identify redundant or unnecessary steps within a process. This type is the most commonly used.



- **Deployment Flowchart** (often called a **swim-lane flowchart**) **-** Shows the actual process flow and identifies the people or groups involved at each step. This type of chart depicts where the people or groups fit into the process sequence, and how they relate to one another throughout the process.



Flowchart Components

The flowchart for specific processes will depict a start-to-finish diagram flow with critical (key) controls highlighted in the body of the map. The process map uses symbols to illustrate various parts of the process flow.

- Rectangles typically represent each step within the process.
- Triangles typically represent additional information relevant to the process.
- Diamonds typically represent each decision point within the process.

When documenting a process or compliance requirement using a flowchart, one should consider the following information:

- Title
- Legend
- Start and end points
- Process or compliance requirement steps
- Decisions and all relevant decision paths
- Responsible parties
- Key risk and controls
- On and off page connectors (where appropriate)
- Notes to provide additional details for the process/control

Narratives

A narrative is a document that describes a process or transaction flow using words rather than a pictorial representation. A narrative may be used either in lieu of a flowchart to document the process or compliance requirement or as a complement to a flowchart to capture additional detail. When documenting a narrative, one must also consider information useful in creating process flows.

Once the process or compliance requirement risk assessment has been completed, the assessment team will document through narratives and/or flowcharts their understanding of the moderate and high risk significant processes. Narratives provide an understanding of a process or compliance requirement and help identify and document key risks and controls as well as control gaps in a process. Narratives provide knowledge that can be used in future years or for other means.

When completing a narrative, consider the following:

- Date when the narrative was prepared and reviewed
- Agency name and location
- Account name or Program/Grant (e.g., Accounts Payable, Federal Pell Grant)
- Significant Process or Compliance Requirement name (e.g., Financial Statement Close Process, Eligibility Requirement)
- Source of information (e.g., process owner's title)
- Purpose (e.g., to document the accounts payable process)
- Background

- Supporting system(s)/Application(s) used
- Process overview or summary
- Input (beginning of process) and Output (end of process)
- Controls
- Cross-reference to flowchart and/or Risk and Control Matrix (RACM)
- Control weaknesses or improvement opportunities

6.4 LEVEL OF DETAIL IN DOCUMENTATION

The primary purpose of the assessment team's documentation is to help identify where operational errors could occur and where controls exist to prevent or detect those errors. The assessment team should not obtain or prepare documentation about every detail of the process or compliance requirement. Not only is excessively detailed documentation very time-consuming and costly to develop, it may be more confusing than helpful to the assessment team members and to others reviewing the documentation.

6.5 FRAMING "RISK QUESTIONS AND STATEMENTS"

The assessment team should identify the points in the flow of transaction where controls are needed by identifying key risks related to what could prevent each control objective from being achieved. For each significant process or compliance requirement, the assessment team should identify the points within the flow of transactions where data is initiated, transferred, or otherwise changed and where there can be a failure to achieve the relevant financial statement assertions or compliance with laws and regulations. These are points where controls are needed.

For each control objective, the assessment team should develop a list of the important errors which could cause a failure to achieve the objective. The team may choose to frame these points as questions or as statements (e.g., "What ensures that correct sales prices are used on the invoice?" or "Incorrect unit sales prices are used on the invoice."). Some examples are listed below in the Risk Chart. Refer to the Financial Statement Assertion Risk Guidance (Addendix 4.2C) and Compliance Internal Control Guidance (Addendix 4.2D).

Questions or statements are formulated by reference to the flowcharted transaction flow (or narratives), and generally focus on the points where data is initiated, authorized, recorded, processed and reported. In some cases, it may be more efficient to begin at the end of the processing stream and work backward to its origin.

Illustrative *"Risk"* Questions

(for two financial statement assertions in context of a hypothetical purchasing process)

Financial Statement Assertion: ***Completeness***

- What ensures that all purchases received are recorded in the purchase status file?
- What ensures that all vendor invoices are recorded in the invoice register?
- What ensures that items marked "received" in the purchase status file are included in the month-end accrual?

Financial Statement Assertion: ***Existence***

- What ensures that purchases are not recorded as received in the purchase status file when not actually received?
- What ensures that vendor invoices are not recorded in the invoice register as paid when not actually paid?
- What ensures that the purchase order status is updated in the purchase status file when invoices are recorded?

Illustrative *"Risk"* Questions

(for two compliance requirements in context of a hypothetical Federal Grant)

Compliance Requirement: ***Allowable Costs/Cost Principles***

- What ensures that all purchases are compared to the list of allowable and unallowable expenditures?
- What ensures that there is adequate segregation of duties in review and authorization of costs?
- What ensures that a comparison is made with budget and expectations of allowable costs?

Compliance Requirement: ***Eligibility***

- What ensures the accuracy and completeness of data used to determine eligibility requirements?
- What ensures the calculation of eligibility amounts is consistent with program requirements?
- What ensures limited access to eligibility records?

The assessment team may find that the questions are best developed in a group brainstorming exercise. The team will often find that process owners are an excellent source of ideas for "what could go wrong" as well.

The team should exercise professional judgment in identifying potential errors of significance. It is rarely practical, useful or cost-effective to identify or evaluate controls with respect to ***every*** conceivable error; consideration of the financial statement risk and compliance requirement should be made.

6.6 CREATING THE RISK AND CONTROL MATRIX

The **Risk and Control Matrix** is a common format for documenting the assessment team's analysis of "what could go wrong," and subsequently, the controls in place to prevent or detect those risks.

The Risk and Control Matrix is designed to capture, for each significant process or compliance requirement (or transaction type, if necessary), the following information:

- The significant processes or compliance requirement and risk rating impacting the account or program/grant
- The team's risk questions or statements for each objective of what could go wrong
- Relevant controls in place to prevent those errors or detect and correct them
- A cross-reference to the flowchart, narrative and/or other workpaper describing the control
- Control type (prevent or detect and automated, manual or both)
- Financial statement assertion covered (financial assessment only)
- How often the control is performed

To assist in the preparation and maintenance of the Risk and Control Matrix, see Appendix 6.6A, Financial Risk and Control Matrix and Appendix 6.6B, Compliance Risk and Control Matrix.

Identifying Controls

After completion of process or compliance requirement interviews and documentation of process flows and narratives, the agency should consider controls over each significant process or compliance requirement that address the "what can go wrong" questions for the relevant assertions. The objective is to identify the controls that provide reasonable assurance that errors relating to each of the relevant financial statement assertions are prevented, or that any errors that occur during processing are detected and corrected.

For each "what could go wrong" question, relevant controls should be recorded on the Risk and Control Matrix. Controls should be identified by description and by reference to flowcharts/narratives; controls frequently apply to more than one question/risk, and can be cross-referenced within the Risk and Control Matrix as well.

Management generally designs, and places into operation, controls over processes to confirm that the operating, financial reporting, and compliance objectives of each process are achieved. Therefore, the agency should identify controls related to the initiation, recording, processing, and reporting of transactions.

In some situations, the agency may identify entity-level controls that are relevant to operating, financial reporting and compliance objectives. If these entity-level controls are sufficiently sensitive to prevent or detect errors of importance for one or more assertions, the agency may identify and evaluate them. While entity-level controls may be present, the assessment team should not focus solely on such controls because they generally are dependent on controls over

processes or activities at the transaction level. The assessment team should also understand processes or activities at the transaction level in order to identify and understand controls that address all risks. The agency's conclusions about the effectiveness of the related controls may be based on a combination of entity-level controls and controls at the transaction level (refer to Chapter 5 – Introduction to Processes and Controls).

The assessment team should keep in mind that, to be effective, internal controls often have to include strong prevent controls in addition to detect controls. For example, where there is a high volume of transactions, the lack of prevent controls significantly increases the risk of errors and accordingly increases the need for particularly sensitive detect controls. In the absence of prevent controls, a high number of errors can render detect controls ineffective in detecting and correcting errors in a timely manner. The categorization of a control by the assessment team may depend on how and for what purpose it is used, and the way in which the agency views it. Ultimately, what matters is not the categorization but whether the control is effective in reducing the risk of errors of importance or fraud.

IT Control Considerations

Prevent and detect controls can reside both within and outside of computerized environments. Within the computerized environment, prevent and detect controls are often referred to collectively as "application controls" in that their implementation and ongoing effectiveness depends on the consistent application of an embedded software program or application to transactions processed by that application. Programmed controls usually are either programmed procedures (e.g., edit, matching, or reconciliation routines) or computer processes (e.g., calculations, on-line entries, automatic interfaces between systems). Identifying controls may require collaboration with both process owners and IT personnel.

If the agency determines that management is relying on programmed controls or that identified controls are dependent on IT-generated data (i.e., electronic evidence), it should ask a second question: "What ensures that programmed controls are operating effectively?" The response may be:

1. User procedures verify the accuracy of the processing (e.g., manually recomputed complex calculations or reconcile IT reports to manual batch totals) and/or
2. Management relies on the IT system to effectively execute the control or produce the data.

When (2) is the response, the agency should consider the effect of IT general controls in evaluating the effectiveness of controls that are dependent on the IT system or IT-generated data. IT general controls are IT processes and related controls that generally are applied above the computer application level; however, they can be performed on a single platform for a single application. IT general controls, or IT process controls, are designed to: confirm that changes to applications are properly authorized, tested, and approved before they are implemented, and confirm that only authorized personnel and applications have access to data, and then only to perform specifically defined functions (e.g., inquire, execute, update). Except in certain rare instances, agencies will find it necessary to document IT general controls. Many prevent controls are programmed controls residing in computer applications, and detect controls often

rely on information produced by computers. Therefore, the documentation and evaluation of IT general controls is important because those controls provide a basis for concluding that prevent controls residing in computer applications continue to function over time and provide, in part, a basis to rely on the output from computerized applications (i.e., electronic evidence) used in the performance of detect controls.

Most prevent controls residing in computer applications should have been tested prior to implementation. If this is the case and the earlier tests results were retained (and IT General controls prove to be effective), assessment teams generally will be able to document the prevent controls without extensive additional effort.

Considerations for Documenting Controls

The assessment team's documentation of controls should provide evidence that appropriate controls have been established and are effectively designed to prevent or detect errors of importance or fraud. It is recommended the documentation include a description of each control, including how the control is performed, who performs the control, what data reports, files, or other materials are used in performing the control, and what physical evidence, if any, is produced as a result of performing the control. This documentation will be helpful in subsequent phases of the process, particularly in designing procedures to verify the operating effectiveness of those controls. In addition, this documentation will be useful in:

- Identifying whether controls have changed over time.
- Identifying situations where there is a potential lack of segregation of duties.
- Considering whether controls have been designed so that they are not easily overridden and, if they are overridden, whether policies and programs (e.g., fraud programs) exist to detect and report such overrides.

The following questions should be considered when documenting controls:

- How?
  - How is the control performed?
  - How does one know when the control is not working? (Be specific and include details of report names or systems used.)
- What?
  - What does the control seek to do?
  - What is the frequency of the control (e.g. daily, annually)?
  - What is the evidence that the control is working?
- Who?
  - Who performs the control? (Use job titles.)
  - Who performs the control in the person's absence?
- When?
  - When is the control performed? (Are there any dependencies which must be performed prior to the control operating? Can the control be bypassed and processing continues?)

Determining the "Right" Combination of Controls

A Top-Down, Risk-Based approach first considers entity-level controls and then transaction-level controls. When selecting the "right" combination of controls, agencies should select a combination of prevent and detect controls that were clearly understood and preliminarily evaluated to mitigate the risks for relevant financial statement assertions and compliance requirements. When considering the "right combination of controls", it is important to select those prevent and detect controls that are sufficiently sensitive by themselves or in combination with other controls to mitigate the risks of a material misstatement or noncompliance with laws and regulations.

From a testing perspective, selecting the "right" combination of controls can be very important. Typically, manual prevent controls can be difficult to test because agencies will need to test a higher number of occurrences in order to determine that the controls operated effectively. However, when selecting controls to test, agencies should keep in mind that detect controls often work in combination with prevent controls to mitigate the risks of material misstatement or noncompliance (i.e., rely on the accuracy of underlying data, which is the result of effective prevent controls). Therefore, agencies need to test the most efficient combination of both prevent and detect controls, whether manual, IT-dependent manual, application or related IT general controls. Testing application controls, however, may be more efficient because agencies may only have to test a sample of one of each applicable transaction type to determine that they operated effectively, provided the agency can conclude that IT General Controls supporting the application controls are functioning effectively.

The level of financial reporting or compliance risk identified by management can have a direct influence on how persuasive the evidence needs to be for identified controls in each area. By using this top-down, risk-based approach, and identifying the "right" combination of controls, testing efforts can be varied to direct increased levels of testing to higher risk areas and related controls, thus reducing the need for more extensive testing and documentation of lower risk areas and related controls (see Chapter 7 – Testing Theory and Strategy for further discussion).

6.7 REVIEWING UNDERSTANDING WITH THE PROCESS OWNER

Once the assessment team has completed its detailed control evaluation, the results of the analysis should be reviewed with the process owner. The purpose of this review is two-fold:

1. To confirm that the assessment team understands the process and compliance requirements and controls are accurate and complete.
2. To improve the process owner's awareness and understanding of key risks and the effectiveness of the controls in reducing risk.

Depending on the process owner's experience and perspective, it may be helpful for the assessment team to provide some general background on internal controls. The team should generally share flowcharts and control analyses with process owners, confirming the team's understanding and discussing the team's views on the effectiveness of the control system and opportunities for its improvement. The results of the meetings should be documented in the

workpapers, and any questions or issues arising from them resolved to the assessment team's satisfaction.

6.8 WALKTHROUGHS

Perform Walkthroughs to Confirm Understanding of Processes/Compliance Requirements and Controls

Once the process or compliance requirement risk assessment has been completed, the assessment team will perform walkthroughs of the moderate and high risk significant processes or compliance requirements in order to confirm the teams understanding of the processes or requirements and the related risks and controls. A walkthrough traces one representative transaction through a process from beginning to end. These walkthroughs should be performed from the point at which the major classes of transactions are initiated to the end of the recording process, to confirm (1) the understanding of the procedures, (2) the correctness of the information obtained about the relevant prevent and/or detect controls in the process, and (3) that these controls have, in fact, been placed in operation. For non-routine and estimation transactions, generally the assessment team can gain an understanding of the transaction, identify and understand controls, and conduct walkthroughs simultaneously.

A walkthrough is normally performed using documents that the assessment team believes are typical of the process or compliance requirement being reviewed. It is recommended to perform a walkthrough for at least one transaction within each significant process or compliance requirement previously identified, unless additional walkthroughs are needed to confirm the assessment teams understanding. When there have been significant changes in the process and/or the supporting computer applications during the period under evaluation, the assessment team should consider the need to walk through transactions that were processed both before and after the change. The need to do this depends on the nature of the change and how it affects the likelihood of errors of importance or fraud in the related accounts.

During the walkthrough, the assessment team should question personnel at each point where important controls or procedures are prescribed (i.e., those most relevant to the accuracy of the financial statements). The questions should focus on the personnel's understanding of what is required and whether the procedures and controls are performed on a regular basis.

The assessment team may also attempt to corroborate information obtained at various points in the walkthrough by asking personnel to describe their understanding of the previous and succeeding process or control activities and to demonstrate what they do. Furthermore, during the walkthrough it is recommended to attempt to identify exceptions to the prescribed processing procedures and controls as well as any differences between what the assessment team understands is required and what is actually done. If the control is an employee review, for example, and the employee is required to initial a document as evidence of having reviewed it, it is recommended to inquire about the nature of the review performed and ascertain whether the documents subject to the walkthrough have been initialed by an appropriate employee. Furthermore, it is important to ask what the person does if the review process reveals an error or other discrepancy in the document, and if appropriate, examine documents where problems were

detected to confirm that appropriate actions were taken. If the control consists of the preparation and analysis of a periodic reconciliation, it is recommended that one should:

- Review one or more of the reconciliations to determine whether all the relevant data are accurately and promptly included.
- Note the disposition of any unusual items.
- Inquire about the actions taken when the reconciliation reveals actual or potential errors.
- Inquire how the errors occurred.
- Whenever practicable, obtain evidence of the correction of the errors that were noted during the reconciliation process.
- Determine whether the reconciliation is performed by or relies on information processed by a computer system. If the reconciliation relies on an automated process, the agency should consider the results of procedures performed related to IT general controls.

In addition to walking through the physical flow of documents and forms, the assessment team should also follow the flow of data (flowchart) and information through the automated processes (at a system level, not a detailed logic level). These procedures may include inquiry of independent and knowledgeable personnel, review of user manuals, observation of a user processing transactions at a terminal in the case of an online application, and review of documentation such as output reports.

Performing Walkthroughs of IT General Controls

IT general controls are designed to (1) ensure that changes to applications are properly authorized, tested, and approved before they are implemented and (2) ensure that only authorized persons and applications have access to data, and then only to perform specifically defined functions (e.g., inquire, execute, update). The assessment team should perform walkthroughs of the IT general controls (or equivalent procedures) to confirm the team's understanding of the IT general controls' design and determine that the controls have been placed into operation. In addition, the assessment team should also obtain evidence about whether the controls are operating as designed. The means of gathering evidence during the walkthroughs or equivalent procedures may include:

- Corroborating the understanding obtained from the IT process owner.
- Selecting an item over which the controls are designed to operate (e.g., a request for a program change) and inspecting evidence of the operation of the controls on that item.
- Using judgment to determine the adequacy of the evidence collected.
- Examining documentation of the control's design.
- Examining reports of key performance indicators or other information that is used to monitor the controls.
- Observing whether the IT process owner or others act upon the results of the controls.

Considerations for Documenting Walkthroughs

Walkthroughs of processes and compliance requirements and the related controls are generally documented in brief memos describing the procedures performed by the assessment team to confirm its understanding of the process design and related controls and whether they have been

placed in operation (refer to Appendix 6.8A, Financial Walkthrough and Appendix 6.8B, Compliance Walkthrough).

6.9 CONTROLS RESIDING OUTSIDE THE AGENCY

Because agencies may use service organizations to hold assets, execute transactions and maintain related accountability, or record transactions and process related data, the assessment team may identify parts of the process and/or controls related to significant accounts or groups of accounts that are performed by service organizations. Additionally, because agencies use central management agencies to provide services that impact the agency's internal control environment, the assessment team may identify parts of the process and/or controls that are performed specifically by the central management agency as part of their services.

Determining Controls Residing Outside the Agency

Service Organizations are third-party service providers performing specific tasks or replacing entire business units or functions of an entity. Some examples of service organizations are:

- Payroll Services (ADP, Ceridian)
- Data Center Hosting (Cimco)

Central Management Agencies are agencies within the State of North Carolina, providing services that impact other agencies' (user agencies) internal control environment. Typically, there are two main types of central management agencies:

- Agencies that assist other agencies with initiating, authorizing, recording, and processing transactions.
- Agencies that host or support other agencies' hardware and/or software.

Some examples of central management agencies would be the Department of State Treasurer, the Office of Information Technology Services, the Office of State Budget and Management, the Office of the State Controller, the Department of Administration, and the North Carolina Community College System Office. These agencies are considered to be central management agencies because they provide services for other agencies that ultimately affect their internal control environment.

When determining the controls residing outside of the agency, it is important to inventory critical outsourced processes, applications, and IT systems. This inventory will act as a starting point in determining the amount of information needed from the specific service organization or central management agency. Refer to Appendix 6.9, for the Service Provider Inventory template. This template will assist the agency in identifying these outsourced items. After the agency completes the inventory document of relevant third-party service organizations and central management agencies, the agency would need to understand how the relevant central management agencies' processes, applications, and systems are controlled. Additionally, the agency would need to understand how any relevant third-party service organizations control their processes, applications, and systems in order to determine if a SOC 1 and/or SOC 2 is needed (refer to Evaluating Use of Work of Others section below for more information).

SOC 1 and SOC 2 (Service Organization Control) replaces SAS 70 (Statement on Auditing Standards No. 70). An SOC 1 Report is a report on controls at a Service Organization which are relevant to a User Organization's internal control over financial reporting. An SOC 1 Report should be performed for third-party service organizations that execute transactions and/or maintain accountability for clients, record transactions and process related data of clients, or develop and sell/lease software that processes transactions of financial significance. The SOC 2 Report was put in place to address demands for assurance over non-financial controls. The SOC 2 Report focuses on controls as they relate to security, availability, processing integrity, confidentiality, and privacy of a system.

SOC 1 and SOC 2 Reports consist of two types:

- Type 1 Report, also called a *Report on management's description of a service organization's system and the suitability of the design of controls*
    - Description of controls that may be relevant to a user organization
    - Controls suitably designed to meet stated control objectives
    - Controls placed in operation (walkthroughs only)
- Type 2 Report, also called a *Report of management's description of a service organization's system and the suitability of the design and operating effectiveness of controls*
    - Controls that were tested were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the related control objectives were achieved during the period specified.
    - Should cover a period of 6 to 12 months
    - The as-of date should be sufficiently close to the user organization's year-end to provide assurance as to the effectiveness of controls at year-end.

Note: Type 2 reports are required in the majority of situations, as Type 1 reports do not include testing of operating effectiveness for the defined service organization controls.

Agencies should consider the following factors when determining the significance of the Service Organization:

- The nature and materiality of the transactions or accounts affected by the service organization. Even if not material to financial statements, the user agency may still need to gain an understanding of the nature of the processes in place at the service organization.
- Significant impact of the services provided to the user agency's internal control system.
- The degree of interaction between internal control at the user agency and the controls of the service organization.

The user agency should first determine whether it has implemented effective internal control over the processing performed by the service organization. In situations where this is the case, the assessment team may not need to gain an understanding of the flow of the transactions or the controls at the service organization because the agency has the ability to, and has, placed effective controls into operation (e.g., comparison of input to output).

When determining controls residing outside of the agency, but within the State of North Carolina, it is important to maintain direct communication with the applicable central management agency to discuss scope and reliance of controls. It is important for the agency to determine all services that would be considered part of the user agency's transaction processing / information system, because these services would be included within the central management's agency scope of internal control testing. Additionally, the central management agency should prepare a description of all applicable controls with sufficient detail for the user agency to plan its own control approach (i.e., help the user agency determine what controls can be relied upon and what controls need to be independently tested.)

Evaluating Use of Work of Others

When an agency uses a service organization, transactions that affect its financial statements or ensures compliance with laws and regulations are subjected to controls that are, at least in part, physically and operationally separate from the agency. The significance of the controls of the service organization to those of the agency depends on the nature of the services provided by the service organization, primarily the nature and materiality of the transactions it processes for the agency. In order for the agency to rely on the controls over the service organization's activities, the agency would need to gain an understanding of the flow of transactions and the controls at the service organization, as well as at the agency. For relevant third-party service organizations, the assessment team should obtain, read, and evaluate an appropriate service auditor's report (i.e., SOC 1/SOC 2, Type 2 Report) that describes the service organization's processes, identifies the related controls, including describing tests of their operating effectiveness performed by the service auditor, and specifies the period covered by the report. The agency should document its conclusions as to how the controls at the service organization support the relevant financial statement assertions (similar to how it documents other controls).

The user organization (agency) should then evaluate the obtained SOC 1/SOC 2, Type 2 Report for appropriateness. In order to properly evaluate the report, the agency should complete the Reliance on the Work of Others template (refer to Appendix 6.9) and look for the following in the report:

- Applications and locations covered by the report
- Flow of significant transactions through the service organization
- What could go wrongs (WCGWs)
- Description of controls
- Service auditor understanding of subject matter
- Timing of service auditor's report
- Service auditor's opinion
- Nature of exceptions noted

After the agency evaluates its third-party service organizations, they should then determine whether the agency has implemented effective internal control over the processing performed by the relevant central management agencies. In order to evaluate the internal controls of the central management agency, the user agency should obtain test results from the central management agency and map the central management agency's internal controls to the user agency's controls.

After the user agency performs this mapping, they should determine if any additional controls may be needed at the user agency to achieve an appropriate level of control. Once the user agency determines that no additional controls are needed and that the central management agency has an effective internal control environment, the agency should then complete the Reliance on the Work of Others template (refer to Appendix 6.9). Once this template is completed, the agency can move on to finalizing the documentation of controls.

Note: All control testing documentation would include control activities, test results, and complimentary controls at the user organization. All exceptions noted (on the applicable SOC 1/SOC 2, Type 2 Report for third-party service organizations or on the issue summary report for central management agencies) should be maintained and documented by the user agency and identified within their issue summary template (refer to Chapter 7 for more information on documenting issues).

6.10 FINALIZING THE DOCUMENTATION OF CONTROLS

As the assessment team finalizes its documentation of controls identified over a specific process or compliance requirement, it needs to determine whether (1) all significant risks identified as "what can go wrong" questions are addressed by one or more of the identified controls, and (2) whether the controls that address the identified risks are adequately designed to prevent or detect errors of importance or fraud.

The assessment team should be mindful that it is common for some controls to address more than one risk. For some risks, the assessment team may find it necessary to identify more than one control to conclude the controls, in the aggregate, are adequately designed to address the risks of errors identified. When it is unable to conclude that the design of identified controls provides reasonable assurance that errors of importance or fraud will not be prevented or detected on a timely basis, the assessment team will need to follow-up to confirm appropriate corrective action is taken.

7. TESTING THEORY AND STRATEGY

7.1 INTRODUCTION

After the foundation of the "right" control set has been identified, a testing strategy including evidential matter needed to support management's assessment is developed. This is where the results of the top-down, risk-based assessment and "right" combination of controls culminate.

This phase commences with a listing of controls or combination of controls that address identified financial reporting or compliance risks. These are the controls that the risk assessment team determines to be necessary to adequately address identified financial reporting or compliance risks that may lead to a material misstatement in the financial statements or noncompliance with laws and regulations.

In previous steps of the top-down, risk-based approach, the agency determined which controls address the significant risks identified. The agency has also determined whether the controls are adequately designed to prevent or detect errors of importance or fraud (i.e., walkthroughs – refer to Chapter 6). Once it has been determined that the critical controls are adequately designed, to demonstrate effective internal control, management should determine whether the organization's controls are operating effectively. The agency should retain evidence of this testing to support management's assessment of internal control.

The objectives in performing tests of controls generally include determining all of the following:

- The control is operating as understood and as designed.
- The control is operating throughout the period of review.
- The control is applied on a timely basis.
- The control is applied consistently, on all applicable transactions.
- Errors identified by a control are corrected.

Tests of controls are directed toward confirming that critical controls operated in an effective manner, as designed, and consistently throughout the period under review. Controls should be tested by someone other than the individual who performs the control.

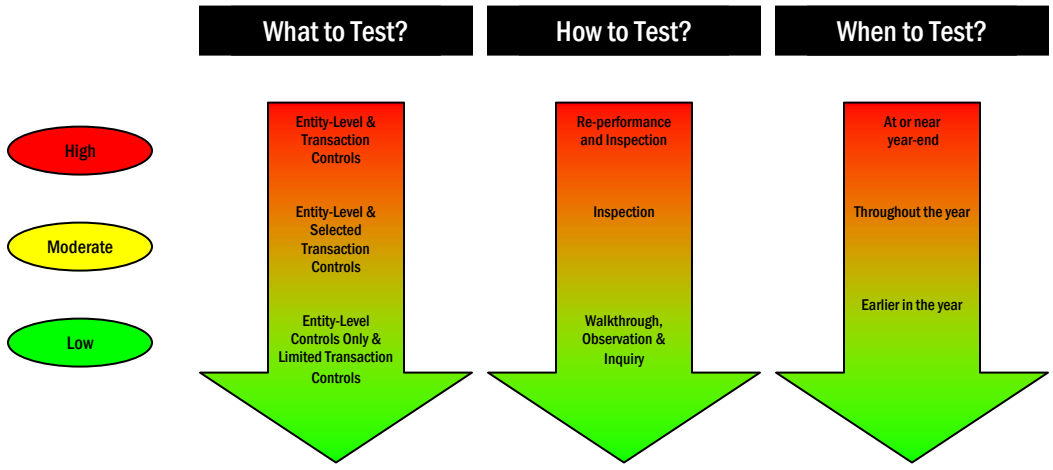
When testing controls, the following steps are performed:

- Determine the nature, extent, and timing of testing of critical controls as part of the testing strategy.
- Execute tests of controls and document in the test plan and detailed workpapers.
- Discuss and document any issues arising from testing and conclude on results.

7.2 DEVELOPING CONTROL TESTING STRATEGIES

The first step in developing the control testing strategy is to determine which controls to test. When selecting controls to test, the agency should consider which controls must operate together to mitigate the risk and whether each control needs to be tested or whether there is a critical control which should be tested. Note too, that each critical control need not be tested *individually***,** particularly if more than one control covers the same risk or if a single test can provide evidence with respect to more than one control. Redundant controls should be discussed further with management. Some level of redundant controls may be considered in the event that the originally tested control fails.

The level of identified risk will help influence the appropriate nature, extent, and timing of the testing to be performed on identified controls. The control testing strategy is a critical step in the top-down, risk-based approach. The level of financial reporting and compliance risk identified by management can have a direct influence on how persuasive the evidence needs to be for testing identified controls in each area. As the risk associated with a control increases, management may need to obtain more persuasive evidence in support of their assessment. The persuasiveness of evidence is not only a function of the quantity of evidence generated, but of its quality. Quantity relates to the sample sizes, which can be varied based on risk when direct testing is performed. Quality of evidence is a function of many factors, including the objectivity and competence of those performing the control, nature of testing performed and review period covered. By using this top-down, risk-based approach, testing efforts can be varied to direct increased levels of testing to higher risk areas and related controls, thus reducing the need for more extensive testing and documentation of lower risk areas and related controls. This offers management an opportunity to adopt an effective testing strategy that considers the benefits, costs and desired return. The graphic below illustrates how the testing strategy can be varied based on the outcome of the risk assessment.



- Sample sizes may also vary based on risk

To develop the testing strategy, the agency should consider "How to Test" (i.e., nature – "N"), "What to Test" (i.e., extent – "E"), and "When to Test" (i.e., timing – "T"). The nature of testing refers to the testing method that most effectively achieves the level of persuasiveness of evidence required to support management's assessment. The extent of testing refers to how much to test and varies according to a variety of factors described in subsequent chapter sections. The timing of test of controls refers to when to test, depending on the nature of the control and the judgment required. Specific details on each of these concepts (NET) are described below.

It should be noted that professional literature provides a great deal of information on testing techniques. This guidance manual includes a limited discussion of key testing considerations as well as recommended practices. It assumes a basic familiarity with testing principles and statistical methods. If necessary, agency members should refer to other reference materials for a more thorough discussion of the underlying principles and related methods.

Determine "N": Nature of Testing

Once the "right" combination of critical controls has been selected for testing, the second step in developing the control testing strategy is to determine the nature of testing.

The agency can choose from a variety of different and often complementary techniques in obtaining sufficient and competent evidence. These techniques are summarized below:

1. REPERFORMANCE: This test method refers to the repetition of a control performed by an employee or system and provides the strongest level of evidence that the control is operating effectively. It is the reperformance of a control using the original data to verify that the result or outcome mirrors the result of the original operation of the control. Reperformance is particularly useful in testing the accuracy of calculations or counts, but is also useful in evaluating internal controls.

2. INSPECTION AND EXAMINATION: This technique involves inspecting documentation, records, or reports that provide evidence that the control has operated effectively. This may include counting securities or cash to verify existence and proper posting, or tracing certain amounts on reconciliations to gain assurance that they were actually performed.

3. OBSERVATION: Actual observation includes direct visual viewing of employees performing their work, as well as other facts and events. Although the tester must consider the impact of his or her presence, observation can provide important evidence that employees are properly trained and actually execute a process or control as designed.

4. INQUIRY: Employees, management, and third parties are asked about performance of procedures, controls, etc. A tester may ask who prepares a reconciliation, how often it is performed, and how corrections are made. Management may be asked how they verify that reconciliations are performed in an accurate and timely manner. Inquiry by itself is often less reliable than other forms of evidence, and may need to be used in combination with other testing techniques.

5. ANALYTICAL REVIEW PROCEDURES: This technique involves evaluations of financial and operational information made by a study and use of predictable relationships among data points. These procedures can also be used during the planning process to gain a better understanding of the specific account area.

Through earlier work in the assessment process, the tester will have conducted some testing of each critical control, through inquiry, observation, and one or more walkthroughs. In determining the nature of testing to conduct at this stage, the tester must consider the evidence already gathered, the nature and importance of the control, and its objectives in further testing. *In general, inquiry and observation do not provide sufficient evidence that a control operated consistently throughout the period of review*. For most critical controls, it will be appropriate to obtain additional evidence through inspection or reperformance.

In addition, the tester must consider the type of control being tested when considering the nature of testing to be performed. There are two basic types of controls: prevent and detect. Somewhat different testing considerations may apply to prevent than to detect controls.

Prevent Controls

In some cases, prevent controls will provide limited evidence indicating if the control was performed, by whom, or how well. In other cases, there will be evidence that a control was performed (e.g., a signature on a document), but the tester may need to test the validity of the data or reperform the checking routine involved to obtain sufficiently persuasive evidence that the control was effective.

Automated prevent controls often provide better evidence and are more easily tested than manual controls. In some cases, the tester may be able to rely on testing performed during application or pre-implementation reviews; in others, reperformance of the control can be done efficiently using test transactions or other computer-assisted techniques. An example of a prevent control is restricting user access to IT systems.

Detect Controls

In contrast, detect controls are usually supported by physical evidence of their performance, such as monthly reconciliations. The tester should examine evidence that the reconciliation was properly completed and that review and follow-up procedures were carried out.

Detect controls, which are generally applied to groups of transactions, are typically performed less frequently than prevent controls. A high degree of reliability can often be obtained by examining comparatively small amounts of evidence. An example of a detect control is performing a monthly bank reconciliation.

Determine "E": Extent of Testing

The first step in determining the extent of testing has already been completed by identifying the "right" combination of controls to test (i.e., what combination of entity-level controls and transaction-level controls is appropriate based on the risk assessment). There are other factors to consider in determining the extent of testing as discussed below.

It is critical to note that judgment should be used to determine the extent of testing. At a high-level, the tester should consider the following factors in this determination:

1. The relative importance of the "risk" question from the Risk and Control Matrix, considering transaction volumes and materiality, transaction complexity, regulatory and statutory considerations, and other factors that the tester may determine to be relevant.

2. How often the control is performed. Less monthly reconciliations need to be tested than a control applied separately to each transaction. For a monthly control, it may be sufficient to perform a detailed test of one month and a review of documentation for other months for any unusual issues and evidence the control was applied.

3. Persuasiveness of the evidence produced by the control. If it can be determined with direct evidence that the control was in effect, fewer items may need to be tested.

4. The need to be satisfied that the control operated as intended throughout the period of reliance. When the tester needs to gain assurance that the control operated over a longer period of review, the tester may need observations and evidence produced at different times throughout the period.

5. The purpose of the test. If the primary purpose of the test is to detect errors and the tester expects the population to be nearly error-free, sample sizes will be based on an expected error rate of zero and will generally be small. If the primary purpose is to estimate the extent of errors with greater precision, sample sizes will be larger. As an example, for controls where the number of occurrences ranges from 50 to 250 during the year, the minimum sample size is approximately 10% of the number of occurrences. As such, the sample size typically seen for a manual control performed daily is 25.

6. Other factors that relate to the effective operation of the control. These include the competence of the person performing the control, the quality of the control environment, changes in the system of controls during the period, and unexplained variances and fluctuations in related accounts.

Use of Sampling

Sampling is a broad term that refers to the application of a procedure to less than 100 percent of a total population (total population being either all items within an account balance or class of transactions) to evaluate some characteristic of the balance or class. Sampling may be **statistical** or **nonstatistical**. Conceptually, the same principles apply in either case; the tester must exercise judgment in planning, performing and evaluating a sample and in relating the results from the sample to other evidential matter in forming a conclusion.

For each test, the tester has two initial decisions to make in considering sampling:

1. Is sampling an appropriate strategy?
2. If so, should the sampling be statistical or nonstatistical?

The use of sampling (statistical or nonstatistical) is not required by professional standards or this methodology. However, it is generally the most efficient approach to gathering sufficient, competent evidence about populations where extended testing is needed and 100% testing is not appropriate.

Sampling carries an inherent risk (often referred to as sampling risk) that the tester may reach a different conclusion than would result from testing every item. This risk is inversely related to the size of the sample.

Statistical vs. Nonstatistical Sampling

As noted above, both methods are fundamentally similar in principle and in the steps followed. They differ in that statistical sampling requires the tester to quantify certain factors and to select items randomly; in turn, statistical sampling allows the tester to express the results quantitatively and to measure and manage sampling risk quantitatively as well.

Nonstatistical sampling uses samples which are selected either informally (i.e., without conscious bias in selection) or judgmentally (i.e., the tester decides which items to select based on judgment as to their relevance to the test objective). Results of nonstatistical sampling are not measurable with respect to precision and confidence, although informal samples may be evaluated as though they were randomly selected.

In general, the recommended practice is to use statistical methods for sampling whenever practical to do so. Although the tester should use his or her judgment as to the most cost-effective testing strategy in each instance, **statistical sampling** should be used when:

- The population of items is large (greater than 500 items, for example).
- Measurability of precision and confidence level are required or desired to extend results to the whole population (e.g., in order to estimate the financial impacts of a control weakness).

- Random selection of test items is practical (i.e., every item must have an equal or calculable chance of selection).

Conversely, **nonstatistical sampling** may be preferable if:

- The population is small (less than 500 items).
- Measurability is not required or desired.
- Other evidence indicates that errors are highly unlikely or the tester has prior information as to which items are likely to be erroneous.

In some cases, it may be useful to combine statistical sampling with either nonstatistical sampling or 100% testing. For example, if the tester expects more errors or higher risk in one subset of the population, he or she might judgmentally sample that portion and use statistical methods to test the rest.

General Steps in Sampling

The following steps should be followed in the design and execution of testing using samples, whether statistical or nonstatistical:

Step 1: DETERMINE THE OBJECTIVE OF THE TEST. The objective of every extended test must be clearly specified.

Step 2: DEFINE THE POPULATION. The population defined by the tester must include all items that are related to the objective of the test. The population is made up of individual sampling units that may be individual transactions, documents, customer or vendor balances, or an individual entry. The tester must consider the objective of the test (what am I going to test?) and, secondarily, the efficiency of the test (how are the records maintained?) when defining the sampling unit. In general, a more elementary sampling unit will produce more reliable test results.

The **sample** is a representation of the whole population. The population may be, for example, a listing of all items, a file drawer of documents, or a computer data file. The sample should be complete in all respects and consistent with the objective of the test. For example, if the tester is concerned with all cash disbursements made during a period, the sample should also include all canceled checks from the period rather than just recorded disbursements.

Step 3: CHOOSE A SAMPLING TECHNIQUE. As discussed above, the tester must initially determine whether a statistical or nonstatistical sampling approach will be used for the test. A variety of specific sampling techniques are available to support tests of controls.

Step 4: DETERMINE THE SAMPLE SIZE. Judgment is necessary in determining the sample size. The decision process for determining the sample size is similar for both statistical and nonstatistical sampling. In statistical sampling, the tester will

quantify the relevant factors; in nonstatistical sampling, the factors will be described in a less structured manner.

Sample size is a function of the variability of the population (expressed as an expected error rate in certain sampling techniques), the acceptable level of risk (i.e., reliability or confidence level), the level of tolerable error, and the population size (refer to Appendix 7.1 for detail on Determining Factors for Sample Size).

SAMPLE SIZE GUIDANCE TABLE

Below is the recommended sample size table to be used based on level of risk:

Estimated Population	Frequency of Control	Range of Sample Size	Risk Level		
			Low	Moderate	High
More than 250	More than daily/ Continuous	25	25	25*	25**
61-249	Daily	15-25	15	20	25
40-60	Weekly	5-10	5	7	10
20-39	Bi-Weekly/ Semi-Monthly	3-7	3	5	7
12-19	Monthly	2-4	2	3	4
4-11	Quarterly	2	2	2	2
1-3	Annually	1	1	1	1
N/A	Automated	1	1	3	4

Note 1: The risk assessment of a specific process/compliance requirement is based on the judgment of the tester and is a function of the level of complexity, routineness, centralization, and automation.

Note 2: For controls with a frequency of "As needed" or "Event Based", use the "Range of Sample Size" guidance above that is closest to the estimated population. For example, if a control occurs as needed and the actual or estimated population equals 45 occurrences, then our sample size guidance indicates we should follow the "Weekly" frequency which is the closest estimated population size noted above.

* - During the test of controls, if a weakness of control is identified (i.e.; an exception is noted), you must expand your test sample from 25 to 30. By doing so, you will determine whether this exception was an isolated incident or a weakness of control.

** - During the test of controls, if a weakness of control is identified (i.e.; an exception is noted), you must expand your test sample from 25 to 40. By doing so, you will determine whether this exception was an isolated incident or a weakness of control.

Step 5: DETERMINE THE METHOD OF SELECTING THE SAMPLE. The tester's objective is to select a sample that can be expected to be representative of all items in the population. For a sample to be statistically valid, sampling units must be selected from the defined population so that each sampling unit has an equal (or calculable) chance of being selected.

Step 6: PERFORM THE SAMPLING PLAN. Once the sample has been selected, the tester should perform the test, applying appropriate procedures.

Step 7: EVALUATE THE SAMPLE RESULTS. After the sample units have been tested, the sample results should be evaluated to determine whether the controls operated effectively.

Step 8: DOCUMENT THE SAMPLING PROCEDURES. Sampling procedures should be documented in workpapers.

Determine "T": Timing of Testing

The period of time over which controls should be evaluated is a matter of the tester's judgment. However, it should vary with the nature of the controls being evaluated, the frequency with which specific controls operate and the specific policies that are applied. Some controls operate continuously, while others operate only at certain times. The tester should evaluate controls over a period of time that is adequate to determine whether the controls are operating effectively.

Management has the flexibility to test controls during the year, and to perform update testing if necessary at year-end based on consideration of the risk of control failure and risk that a material misstatement or noncompliance will occur in the event of a control failure. Ongoing monitoring assists in determining that controls continue to function effectively even though time has passed since the controls were subject to direct testing. The timing and frequency of the direct testing should reflect the risks associated with the significant account or program/grant and related assertions and the risk associated with the controls, the influence of entity-level controls, and the strength of ongoing monitoring procedures and the evidence they provided.

7.3 DOCUMENTING TESTING

As can be seen from the preceding material in this chapter, testing requires the tester to make thoughtful decisions and judgments. In general, documentation of testing must be sufficient to achieve two purposes:

- Guiding those performing testing in the execution of the test procedures.
- Providing an adequate record of the tester's work in planning, performing, and evaluating the tests for subsequent use including management's overall assessment of internal control.

To guide the tester in conducting testing, a test plan should be prepared prior to test execution, although test plans may be revised as needed to reflect any changes in test plans that prove necessary. The tester should develop test plans specifically for each process or compliance requirement. Test plans should provide enough detail to guide the execution of the test, without necessarily containing all of the detailed information used in planning the test (e.g., considerations of tolerable error, expected error, reliability level, and other determinants of sample size).

A test plan should be created for each process or compliance requirement. The test plan should be organized to make test execution as efficient as possible, so that tests related to a common sample are grouped together, for example. As tests are completed, results should be recorded on the test plan and cross-referenced to test leadsheets or to other detailed test documentation elsewhere in the workpapers. The elements of a test plan include:

- Significant process/Compliance requirement and risk rating
- Control description and reference number
- Objectives of the test
- Test procedures
- Results of testwork - including results of test
- Conclusion of tested control
- Issue raised with management and any workpaper reference

Preparation and completion of the test plans are the responsibility of the tester, with the guidance and active participation of the assessment team. When testing must address some unusual or difficult issues, the assessment team should guide the tester in selecting an appropriate testing approach.

Before the tester completes the extended testing phase, the assessment team should carefully review the test plans again to make sure that all necessary tests have been appropriately completed and that all objectives for testing have been achieved.

Test plans may be discussed with the responsible process owner after the test plans have been prepared, and before commencing testing. This will increase process owners' buy-in to the testing phase and may identify controls that the process owners know will fail the testing phase. These tests can be recorded as having failed testing and remediation actions agreed without the tests having been performed. This will save a significant amount of time in the testing phase and enable remediated controls to be designed more quickly. Refer to Appendix 7.3A (Financial) and Appendix 7.3B (Compliance) for the test plan.

In addition, a test leadsheet will be created for each control being tested. The test leadsheet serves as the workpaper to evidence testing performed for each control. There can be one test leadsheet for each control or, if testing procedures can be combined, one test leadsheet can include multiple controls.

The following is specific information that will be included on the test leadsheet before the test is performed:

- Financial statement account/CFDA#
- Significant process or Compliance requirement and risk rating
- Control reference number, description, and frequency of control
- Identify if the control is automated, manual or both and if it is a prevent or detect control
- Control owner
- Estimated population - Determine the population size for the period being sampled. This documents the number of transactions (times) when the control should have occurred. When the population consists of different transaction types, it may be appropriate to describe the risk characteristics of each type to help determine the sampling strategy.
- Sample size and selection methodology - Sample approach to be applied – sample size, sampling method, strategy or source of sample. Is the population comprised of one transaction type, or several types? If more than one transaction, is each type subjected to the same control procedure? If not, this impacts whether you may need more than one sample.
- Source of sample test documents (reports or data) - Source documents include specific reports used to perform the testing, including a description of the sampled items (e.g., select aged items over 30 days from the monthly accounts receivable aging report). Also, it is beneficial to include the contact name for obtaining the information.
- Test procedures - A detailed description of the steps performed (i.e., examination of evidence, reperformance, etc.) to determine if the controls are in place and operating as intended.
- Test attributes - Identify the specific characteristics of the items selected. An attribute either exists or does not exist (e.g., supervisor's signature supports the timely review of the submission of the financial statements). It is important to keep the scope in mind when selecting attributes for testing so that only attributes relevant to the scope are tested. Frequently, there are additional attributes that could be tested, but are unrelated to the risks included in your scope.
- Period from which the sample has been selected (e.g., last three months)
- Definition of an exception (e.g., the supervisor did not approve the employee's travel reimbursement request)

The following is specific information that will be included on the test leadsheet after the test is performed:

- Details of any exceptions identified-completed tickmarks
- Root cause analysis of exceptions identified
- Results
- Review and sign off

Refer to Appendix 7.4A, Financial Test Leadsheet and Appendix 7.4B, Compliance Test Leadsheet.

Documentation Standards

Workpapers can be utilized to document the evidence of the work performed. Workpapers should be designed so that someone with minimal knowledge of the process can follow the work performed.

The objectives of workpapers are to:

- Provide the principal support for observations and conclusions.
- Document the planning, performance, and review of work.
- Document whether the objectives and scope were achieved.
- Provide support for the work procedures.

Workpaper Elements

Typically, workpapers contain standard elements which are discussed further below:

Heading

Each workpaper should include a heading, consisting of the name of the organization or activity being examined, the title or description of the area, and date or period covered by the project.

Example: Department of XXX
Accounts Payable
06/30/XX

Cross-Referencing

Cross-referencing on manual workpapers is used to agree a specific number or fact to another workpaper. Cross-referencing is used to ensure:

- The information on one workpaper agrees with another workpaper.
- Each test procedure was performed and documented.

Cross-referencing is done by indicating the workpaper reference of the relating workpapers next to the information being cross-referenced. Cross-referencing should only be done for key information within workpapers.

Source

The source of the information should always be indicated. In many cases, this will become key to facilitating future follow-up of assessments. For example:

Source: Jane Doe, Vice President

Purpose

Each workpaper should include its nature or purpose. This provides the reviewer with an understanding as to the objective of the workpaper.

Sign-Off

Each working paper should be signed (or initialed) and dated by the individuals preparing and reviewing the workpapers. In cases where subsequent adjustments are made, additional sign-offs may be made.

Tickmarks

Testing results should be shown in a standard manner to allow further review and analysis. Generally, this can be completed by using standard tickmarks. Each workpaper should have a legend indicating the tickmarks used and the related meaning. In the legend, be specific when defining the tickmarks being used. For example, "Agreed to supporting documentation" is not specific enough. A better tickmark would be, "Agreed to Report XX, which was generated from System X on xx/xx/xx."

Evidence of Work Performed

The workpapers should record the information obtained, the analyses made and the conclusion reached. The documentation can take several forms. It may include an attribute worksheet (i.e., test leadsheet) which indicates the testing performed in the columns and the items tested in the rows. It may consist of an observation or scanning memo which indicates the work performed but does not detail the items. For example, if the tester reviewed all expense accounts for the first quarter of the year for unusual expenses, it is not necessary to detail every expense account reviewed. It is necessary to indicate clearly the scope of the documentation reviewed and any exceptions.

Statements necessary to summarize the nature and extent of work performed should be consistent with the objectives of the workstep. For example:

- "Based on testing performed to validate the existence and accuracy of [ABC process], we noted no exceptions."
- "We selected 25 invoices out of 1,000 prepared for fiscal year 20XX and noted no exceptions with respect to the procurement process."

The workpaper should provide enough documentation for a third party to reconstruct the work performed.

Conclusions

A conclusion should be documented on each workpaper based on testing results and/or work performed. The conclusion should be designed so that someone with minimal knowledge of the process or compliance requirement can arrive at the same results.

Types of Workpapers

Workpapers may be electronically or manually prepared. In either case, they can consist of flowcharts, process models, and Word or Excel documents.

7.4 EVALUATING RESULTS OF TESTS OF CONTROLS

The tester should evaluate the results of each test against its objectives. If control exceptions have been found (that is, instances in the sample where the control was not applied as intended), each one should be investigated regardless of sample size. It is important to note that once an exception has been identified, it is critical to gain an understanding of the nature of the exception to help determine the root cause. Factors to consider when gaining an understanding of the exception include:

- Is the exception systematic or a one-time occurrence? For example, is the open purchase order report missing approval because the purchasing manager forgot to evidence the approval or because the purchasing manager is new and does not know the need to review and approve the open purchase order report?
- Does the control exception apply to the whole population or particular segments? For example, particular locations or departments do not document the goods received from suppliers.
- When did the exception occur (e.g., during the year or 13th month)?
- Is the control exception one of performance or documentation (e.g., the purchasing manager reviews the changes to the vendor master list but does not evidence approval of the report)?

The tester must be very careful not to dismiss exceptions as random or unique occurrences. With the small sample sizes typically used for tests of controls, every exception must be considered important.

If the tester is satisfied with the results of the test, no further testing should be required to assess the control as effective. "Effective" implies that the internal controls exist that would prevent or detect a control weaknesses in a timely period by employees in the normal course of performing their assigned functions.

If the test does not achieve the desired objectives several options exist:

- Extend testing (in anticipation of not finding another control exception) – In some cases, it may be appropriate to extend testing at the request of management as to the extent and impact of an error. This should be done sparingly and only after prior discussion with the assessment team. Note that, when statistically valid tests have been performed, the tester should be able to project error rates or balances with sufficient accuracy for management. The tester should always document discussions with management of matters arising from testing.
- Consider whether a compensating control is available to test. If another control (or group of controls) can be identified that achieves the same control objective, it should be tested even if not previously considered key.
- Deem the control ineffective. If other controls do not achieve the same objective, the tester should consider the need for procedures to determine or quantify the impact of the exception.

- Consider control remediation and retest the control. Depending on the timing of when the control exception was identified, there may be time to remediate the control and retest in order to achieve a clean sample.

Once control exceptions have been confirmed, they should be clearly documented and communicated to management.

7.5 COMMUNICATING THE RESULTS OF TESTING

Communicating Exceptions

As in every phase of the EAGLE Program, the tester should promptly review results of the testing work and communicate to management. This is particularly important when exceptions have been found, both to inform management of the potential issues and to direct the tester in considering any factors which might help in evaluating the error.

The tester should use an Issue Summary Log to document control exceptions. The template should include the following information:

- Issue
- Risk/Implication of the control exception
- Recommendation for improvement or remediation plan
- Management's response to the control exception and recommendations

See Appendix 7.6A, Financial Issue Summary Log and Appendix 7.6B, Compliance Issue Summary Log.

Once testing is completed, it is recommended that the tester hold a closing meeting to review all open findings with management and the assessment team to reach final agreements on issues, and obtain management action plans for all control issues that may be documented in management's assessment.

Issues raised in testing – whether related to ineffective operation of controls or misstatement of balances – are often significant and should be discussed on a timely basis.

Identifying Matters for Improvement

Over the course of the evaluation process, it is likely the agency will identify areas where controls may require modification or where the assessment team determines certain processes or compliance requirements require control enhancements to respond to new services or emerging risks. The agency might also identify areas where automating manual controls may improve both efficiency and compliance with management's policies or areas where the agency's evaluation of processes and controls identify redundant controls or other procedures that are no longer necessary. The agency should consider the concept of reasonable assurance when evaluating whether suggested improvements should be implemented.

8. PERFORMANCE

8.1 INTRODUCTION

In the previous steps of the top-down, risk-based approach, the agency determined which controls address the significant risks. The agency also determined whether the controls were adequately designed to prevent or detect errors of importance or fraud. The "right" combination of controls were identified and tested. To provide additional support of management's assessment, agencies should complete a review of their performance measures.

Performance measures assist in identifying effectiveness and efficiency of operations. This includes an agency's basic business objectives and missions, such as profitability goals and safeguarding of resources. Performance measures are tools used to assist agencies in understanding, managing, and improving operations. In addition, they create greater accountability and strengthen the results of government through the continuous improvement of efficiency and effectiveness.

Agencies may measure their performance in several different ways:

- Key Measures related to their core missions
- Productivity Measures related to the costs associated with core business functions
- Administrative Measures related to critical management and compliance requirements
- Other Measures related to performance and service functions

Performance measures not only build upon statewide and agency-specific strategic planning efforts to determine a desired direction, but they also involve thorough evaluation of agency progress in a variety of critical areas. These areas include statewide outcomes such as fraud or misappropriation of assets and common administrative tasks such as human resources management. Other key components in performance management include gathering and using reliable data, analyzing the data, communicating the results, and developing and executing a plan for improvement.

8.2 PERFORMANCE MEASURES

Performance measures are an extension of an agency's planning process. After an agency sets its future direction, performance measures look at how well the agency is performing, identify where deficiencies exist, heighten accountability, and communicate the progress throughout the agency. First, agencies should:

- Establish and Update
    - Review current performance measures and update as needed; create new measures where appropriate; and ensure measures flow from the agency's goals.

- Establish Accountability
    - Ensure ownership of each measure is assigned and formalized; identify responsibilities for data collection, reporting, and analysis; and establish reward systems to acknowledge success.
- Collect and Report Data
    - Identify data sources; address reliability, accuracy, and timeliness issues; document data entry, tabulation, and summarization methods for each measure; and design processes to support the collection and reporting data.
- Analyze and Review Performance Data
    - Analyze and validate the results; compare the results with pre-established targets (benchmarks); review results with management; provide feedback to process owners for continuous improvement.

Each year, colleges report on performance measures that the N.C. General Assembly has mandated for evaluating how well colleges are serving students, business and industry, and the community while, state agencies report on performance measures to OSBM on how well they are servicing the citizens of North Carolina. Therefore, for the EAGLE Program, we have created a tool that should be used as a compliment to the already established performance measures.

We have developed the following performance measures:

- General Accounting
- Federal Grants
- Procurement
- Student Financial Aid

For each of these performance measures, agencies will gain insight into areas that may be risky or need improvement.

- General Accounting performance measures analyze the number of days to complete bank reconciliations, the percent of A/P vouchers that are processed using a P-Card or E- payment, the number of days to resolve audit findings, etc. (Appendix 8.2A).

- Federal Grants performance measures analyze the number of days to resolve audit findings for programs/grants, timeliness of reporting requirements, and compliance with monitoring requirements (Appendix 8.2B).

- Procurement performance measures analyze compliance with P & C Rules and Regulations (Appendix 8.2C).

- Student Financial Aid performance measures analyze compliance requirements for student loan and financial assistance grants (Appendix 8.2D).

9. ASSESSMENT, AGENCY SELF-ASSESSMENT

9.1 INTRODUCTION

The EAGLE Program requires each agency to perform an annual assessment of internal control. As part of this assessment process, the Office of the State Controller has developed a series of evaluation tools. The OSC strongly recommends that each agency use these tools to encourage uniformity and consistency in the assessment process.

9.2 EVALUATION TOOLS

In order to complete the Internal Control Self-Assessment, agencies must first identify and evaluate risks and controls that reduce the possibility of material misstatements, misappropriation of assets and noncompliance with laws and regulations. In order to properly identify and evaluate risks and controls, the following evaluation tools are available:

- Financial Materiality and Risk Assessment Example (Appendix 4.1A)
    - This example assists agencies in identifying, understanding and evaluating risk at the financial statement level. Additionally, it assists agencies in identifying accounts and processes that should be included in the scope of the assessment.
- Compliance Materiality and Risk Assessment (Appendix 4.1B)
    - This template assists agencies in identifying, understanding and evaluating risk at the program/grant level. Additionally, it assists agencies in identifying the applicable compliance requirements that should be included in the scope of the assessment.
- Financial Statement Assertion Guidance (Appendix 4.2C)
    - The guidance includes the financial statement assertions that are affected by each of the control questions. When identifying and documenting controls, verify that you have at least one control for each assertion per account/process.
- Compliance Internal Controls Guidance (Appendix 4.2D)
    - This guidance includes a general description of each type of compliance requirement, along with a set of common controls. You may refer to this list when identifying and documenting controls.
- Financial Narrative and Process Flowchart Examples (Appendix 6.1A & Appendix 6.3)
    - These examples assist agencies in understanding and documenting processes. Additionally, they assist agencies in identifying risks, controls and control gaps. Narratives and flowcharts can be used to document and maintain knowledge that may be used in future years by other state employees.

- Compliance Narrative (Appendix 6.1B)
    - This template assists agencies in understanding and documenting compliance requirements. Additionally, it assists agencies in identifying risks, controls and control gaps.
- Financial Walkthrough Example (Appendix 6.8A)
    - This example walkthrough assists agencies in confirming their understanding of the significant flow of transactions (processes), relevant controls and process documentation (narrative or flowchart). The walkthrough is also used to conclude on the effectiveness of the overall design of controls.
- Compliance Walkthrough (Appendix 6.8B)
    - This template assists agencies in confirming their understanding of the compliance requirement, relevant controls and documentation (narrative or flowchart). The walkthrough is also used to conclude on the effectiveness of the overall design of controls.
- IT General Controls (Appendix 5.1A Option 1 & Appendix 5.1B Option 2)
    - The provided templates on IT controls are designed to support financial reporting and compliance objectives limited to only those applications and systems used in the business processes and compliance requirements that were determined to be High or Moderate. Option 1 should be used if the user (agency's IT specialist) is familiar with COBIT standards. Option 2 should be used if the agency is not familiar with COBIT standards.
- Financial Risk and Control Matrix (RACM) Example (Appendix 6.6A)
    - This example RACM assists agencies in documenting risks and controls (type and nature) for each of the financial statement assertions. It also allows agencies to identify control gaps as well as unmitigated risks and assists in developing testing strategies.
- Compliance Risk and Control Matrix (RACM) (Appendix 6.6B)
    - This template assists agencies in documenting compliance risks and controls (type and nature). It also allows agencies to identify control gaps as well as unmitigated risks and assists in developing testing strategies.
- Service Provider Inventory & Reliance on the Work of Others (Appendix 6.9)
    - This template assists agencies in creating an inventory of significant processes performed by service providers (third-party and central management agencies) on behalf of the agency. This template also assists agencies in documenting consideration of the service agencies' internal control effectiveness over the significant process(es).
- Financial Test Plan and Test Leadsheet Examples (Appendix 7.3A & Appendix 7.4A)
    - These examples assist agencies in developing a plan and documenting tests of the operating effectiveness of financial controls in order to determine whether the controls are effectively mitigating risk. Without testing, you are only assessing the adequacy of control design, not the operating effectiveness of the controls.

- Compliance Test Plan and Test Leadsheet (Appendix 7.3B & Appendix 7.4B)
    - These templates assist agencies in developing a plan and documenting tests of the operating effectiveness of compliance controls in order to determine whether the controls are effectively mitigating risk. Without testing, you are only assessing the adequacy of control design, not the operating effectiveness of the controls.
- Sample Size Guidance (Appendix 7.2)
    - This guidance assists agencies in deciding the amount of testing necessary to determine whether the controls are operating effectively in order to mitigate risk.
- Financial Issue Summary Log Example (Appendix 7.6A)
    - This example assists agencies in documenting identified financial statement issues (exceptions) found during walkthroughs (design effectiveness) and testing (operating effectiveness). Additionally, this example allows agencies to document recommendations and remediation plans as they relate to the specific issues identified during the evaluation procedures.
- Compliance Issue Summary Log (Appendix 7.6B)
    - This template assists agencies in documenting identified compliance issues (exceptions) found during walkthroughs (design effectiveness) and testing (operating effectiveness). Additionally, this template allows agencies to document recommendations and remediation plans as they relate to the specific issues identified during the evaluation procedures.
- Performance (Appendix 8.2A, Appendix 8.2B, Appendix 8.2C and Appendix 8.2D)
    - These templates assist agencies in documenting their review of performance measures.

Note: It is required that State Agencies utilize all applicable templates and guidance noted above when documenting and evaluating the internal control environment. Templates are available for download on the EAGLE website.

9. 3 LOADING RESULTS

In order for OSC to provide agency's with feedback, each agency should load all documentation as completed to the EAGLE SharePoint website (via the link located on the Office of the State Controller's EAGLE website: http://www.osc.nc.gov/eagle/).

In order to properly load documentation, agencies should follow the steps noted below:

EAGLE Website Log-in Instructions:

1. In order to log-in, a person must be listed as a User on the EAGLE website.
2. The user name is eagle\ and the user's first initial and last name. Ex. John Smith will have the user name eagle\jsmith. OSC will provide each user with a password.
3. The following is the link to the EAGLE homepage- https://eagle.ncosc.net. This link is included on the EAGLE website shown above.

4. Some Internet Browsers will prompt EAGLE users to install a security certificate before logging into the EAGLE site. The steps to install the security certificate are the following:
    - Click "**Continue to this website not recommended**."
    - Log in with your user name and password as provided above. **Note:** Your user name contains **eagle** (*backslash not forward slash*)
    - Click **"Certification Error"** on the top bar next to URL
    - Click **"View Certificate"**
    - Click **"Install Certificate"**
    - Click **"Next"**
    - Click **"Next"** again
    - Click **"Finish"**
    - Click **"Yes"**
    - Click **"Ok"**
5. Type in your **"User Name"** Ex. eagle\jsmith.
6. Enter your password and click **"OK"**.
7. Now that you have entered the website, please change your password with the link in the top right.
8. The links on the left and the top will guide you to important information and materials.
9. Use the folder labeled, **"Templates to download"** located on the left, to gather the necessary templates to start with the assessment. Directions for downloading and uploading documents are located on the left and in the announcements folder.

Downloading a document:

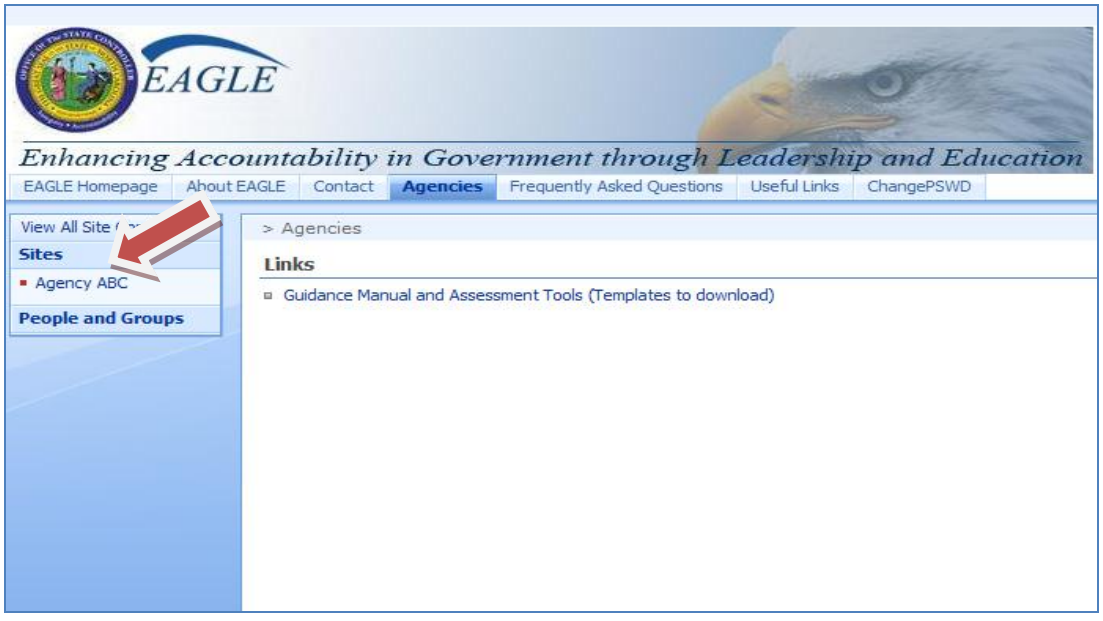
1. From the EAGLE Homepage click the link **"Guidance Manual, Assessment Tools (Templates to download)"**, & **"Visio Video (Flowcharting program)"**.
2. Place cursor on the document you want to download and click on the **down arrow** to the far right.
3. Scroll down to **"send to"** and click **"download a copy"**. Click **"Open."**
4. This document is now free to be modified and saved on your hard drive/network drive.
5. When saving this document remember the location of the file to help with the uploading process.

Uploading a document:

1. From the EAGLE Homepage, click the link that represents your entity type. This is located on the top link bar and will be **"Agencies"** or **"Colleges"** depending on your entity type.
2. Click your entity's name under sites.
3. Click on your entity's document folder. For example: OSC's documents.
4. Click on the arrow for **upload** document. There are 2 options, **Upload document** or **Upload multiple documents**. The user can use either option.
5. Click **"Browse"** to find the file that you want to upload. Select the file, click **"Open"** and then click **"OK."**

6. The file is now uploaded to your entity's folder. (Note to user: **Overwrite existing files** is clicked by default. When this option is clicked, the new uploaded file will save over any previous files in your document folder that have the same file name as the new uploaded file.)

The following screenshots depict the EAGLE website maneuverability for an **example agency.**



9.4 NEXT STEPS

After all documentation is loaded by the Agency into the EAGLE SharePoint site, the Office of the State Controller will aggregate the results for the various agencies and review the results as part of their independent assessment.

10. FRAUD CONCEPT

10.1 INTRODUCTION

Throughout the EAGLE Program, the importance of fraud should be a factor in planning, executing, and evaluating the assessment of the internal control program. Elements of an anti-fraud program include: setting the proper tone within the organization, proactively identifying fraud risks and monitoring internal controls to prevent or detect fraud, and establishing reactive protocols in the event that fraud is suspected.

The risk of fraud can be reduced through a combination of prevention, deterrence, and detection measures. However, fraud can be difficult to detect because it often involves concealment through falsification of documents or collusion among management, employees, or third parties. Therefore, it is important to place a strong emphasis on fraud prevention, which may reduce opportunities for fraud to take place, and fraud deterrence, which could persuade individuals not to commit fraud because of the likelihood of detection and punishment. Moreover, prevention and deterrence measures are much less costly than the time and expense required for fraud detection and investigation.

An agency's management has both the responsibility and the means to implement measures to reduce the incidence of fraud. The measures an organization takes to prevent and deter fraud can also help create a positive workplace environment that can enhance the agency's ability to recruit and retain high-quality employees.

Documentation of processes and controls as well as tests of controls should provide evidence that appropriate controls have been established and are effectively designed to prevent or detect errors of importance or fraud. Specifically, management should consider if there are controls to sufficiently address identified risks of material misstatement or noncompliance due to fraud and the risk of management override of other controls. Controls that might address these risks include:

- Controls over significant, unusual transactions, particularly those that result in late or unusual journal entries;
- Controls over journal entries and adjustments made during the 13th month financial reporting process;
- Controls over related party transactions;
- Controls related to significant management estimates; and
- Controls that mitigate incentives for, and pressures on, management to falsify or inappropriately manage financial results.

As such, management's evaluation of the risk of misstatement or noncompliance should include consideration of the vulnerability of the agency to fraudulent activity (e.g., fraudulent financial reporting, misappropriation of assets and corruption, and whether any such exposure could result in a material misstatement of the financial statements or noncompliance with laws and regulations).

10.2 FRAUD DEFINED

Definition

Misstatements in the financial statements and noncompliance with laws and regulations can arise from fraud or error. The distinguishing factor between fraud and error is whether the underlying action that results in the misstatement or noncompliance is intentional or unintentional.

The term "fraud," according to Statement on Auditing Standards (SAS) 99, *Consideration of Fraud in a Financial Statement Audit*, is defined as an intentional act, performed by one or more individuals among management, employees, or third parties, that results in a material misstatement in the financial statements that are the subject of an audit. Although fraud is a broad legal concept, an internal control framework is established to help prevent or detect fraud that may cause a material misstatement in the financial statements. Fraud involving one or more members of management or those charged with governance is referred to as "management fraud;" fraud involving only employees of an organization is referred to as "employee fraud." In either case, there may be collusion within an organization or with third parties outside of an organization.

The term "error" refers to an unintentional misstatement in financial statements, including the omission of an amount or a disclosure, such as the following:

- A mistake in gathering or processing data from which financial statements are prepared.
- An incorrect accounting estimate arising from oversight or misinterpretation of facts.
- A mistake in the application of accounting principles relating to measurement, recognition, classification, presentation or disclosure.

Types of Fraud

The two primary types of intentional misstatements relevant to an internal control framework are misstatements resulting from misappropriation of assets and misstatements resulting from fraudulent financial reporting. Corruption is sometimes described as a third type of fraud to highlight the abusing influence and power within an organization to obtain a benefit at an organization's expense. Examples might include kickbacks or conflicts of interest.

Misappropriation of assets involves the theft of an agency's assets and is often perpetrated by employees in relatively small and immaterial amounts. However, it can also involve management who are usually more able to disguise or conceal misappropriations in ways that are difficult to detect. Misappropriation of assets can be accomplished in a variety of ways including:

- Embezzling cash receipts (for example, misappropriating collections on accounts receivable or diverting receipts for written-off accounts to personal bank accounts).
- Stealing physical assets or intellectual property (for example, stealing inventory for personal use or for sale, stealing scrap for resale, colluding with a competitor by disclosing technological data in return for payment).

- Causing an agency to pay for goods and services not received (for example, payments to fictitious vendors, kickbacks paid by vendors to the agency's purchasing agents in return for inflating prices, payments to fictitious employees).
- Using an agency's assets for personal use (for example, using the agency's assets as collateral for a personal loan or a loan to a related party).

Misappropriation of assets is often accompanied by false or misleading records or documents in order to conceal the fact that the assets are missing or have been pledged without proper authorization.

Fraudulent financial reporting involves intentional misstatements including omissions of amounts or disclosures in financial statements to deceive financial statement users. Fraudulent financial reporting may be accomplished by the following:

- Manipulation, falsification (including forgery), or alteration of accounting records or supporting documentation from which the financial statements are prepared.
- Misrepresentation in or intentional omission from, the financial statements of events, transactions or other significant information.
- Intentional misapplication of accounting principles relating to amounts, classification, manner of presentation, or disclosure.

Fraudulent financial reporting often involves management override of controls that otherwise may appear to be operating effectively. Fraud can be committed by management overriding controls using such techniques as:

- Recording fictitious journal entries, particularly close to the end of an accounting period, to manipulate operating results or achieve other objectives;
- Inappropriately adjusting assumptions and changing judgments used to estimate account balances;
- Omitting, advancing or delaying recognition in the financial statements of events and transactions that have occurred during the reporting period;
- Concealing, or not disclosing, facts that could affect the amounts recorded in the financial statements;
- Engaging in complex transactions that are structured to misrepresent the financial position or financial performance of the agency; and
- Altering records and terms related to significant and unusual transactions.

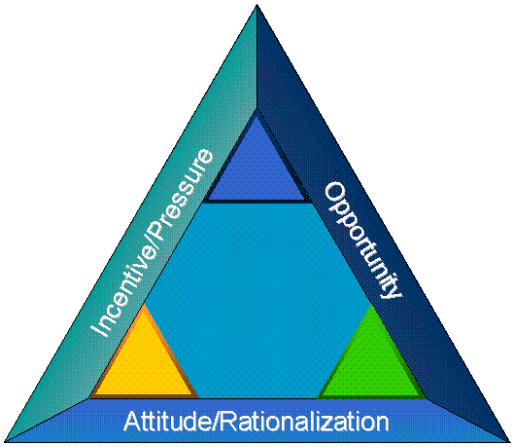
10.3 WHO COMMITS FRAUD AND WHY IS FRAUD COMMITTED

Fraud can occur at any level of the organization. Management might commit fraud via manipulation of the accounting records. Management fraud is typically committed through fraudulent financial reporting. Employees might commit fraud by stealing an organization's assets such as cash, inventory, etc. Employee fraud is fraud perpetrated by employees against the organization.

The Fraud Triangle

The fraud triangle concept is relevant in identifying and understanding the importance of fraud risk factors that may be present. The three conditions typically present when fraud exists are:

- Incentives or pressures on management to perpetrate fraud to achieve desired financial results.
- Opportunity (i.e., control weaknesses) to carry out fraud without being detected.
- Attitude of personnel who are able to rationalize to themselves a need for the fraud (i.e., they convince themselves that the fraud is justified).



The Fraud Triangle

Fraud involves incentive or pressure to commit fraud, a perceived opportunity to do so and some rationalization of the act. Individuals may have an incentive to misappropriate assets, for example, because the individuals are living beyond their means. Fraudulent financial reporting may be committed because management is under pressure, from sources outside or inside the agency, to achieve an expected (and perhaps unrealistic) earnings or operational target – particularly since the consequences to management for failing to meet financial or operating goals can be significant. A perceived opportunity for fraudulent financial reporting or misappropriation of assets may exist when an individual believes internal control can be overridden, for example, because the individual is in a position of trust or has knowledge of specific weaknesses in internal control. Individuals may be able to rationalize committing a fraudulent act. Some individuals possess an attitude, character or set of ethical values that allow them knowingly and intentionally to commit a dishonest act. However, even otherwise honest individuals can commit fraud in an environment that imposes sufficient pressure on them.

It is important to be aware of the incentives or pressures that might lead someone to commit fraud and be alert for indication(s) for potential fraudulent activity. The likelihood of fraud increases when one or more fraud risks have been identified, particularly in an environment where significant pressure exists to meet financial or operational targets. Identifying one or more fraud risk factors does not necessarily mean that internal control at the agency level is ineffective. However, the presence of numerous fraud risk factors should heighten awareness. Particular attention should be paid to risk factors relating to attitudes of management or oversight boards, or opportunities resulting from inappropriate attention to, or disregard for, internal control.

10.4 RESPONSIBILITY TO DETECT FRAUD AND DEVELOPING AN APPROPRIATE OVERSIGHT PROCESS

The primary responsibility for the prevention and detection of fraud rests with both those charged with governance of the agency and with management. The respective responsibilities of those charged with governance and of management may vary by agency. In some entities, the governance structure may be more informal as those charged with governance may be the same individuals as management of the agency.

It is important that management, with the oversight of those charged with governance, place a strong emphasis on fraud prevention, which may reduce opportunities for fraud to take place, and fraud deterrence, which could persuade individuals not to commit fraud because of the likelihood of detection and punishment. This involves a culture of honesty and ethical behavior. Such a culture, based on a strong set of core values, is communicated and demonstrated by management and by those charged with governance. It provides the foundation for employees as to how the agency conducts its business. Creating a culture of honesty and ethical behavior includes setting the proper tone; creating a positive workplace environment; hiring, training and promoting appropriate employees; requiring periodic confirmation by employees of their responsibilities; and taking appropriate action in response to actual, suspected or alleged fraud.

Setting the Tone at the Top

Chief Executive Officers, Chief Financial Officers, Chancellors and Vice Chancellors of agencies set the "tone at the top" for ethical behavior within any organization. Research in moral development strongly suggests that honesty can best be reinforced when a proper example is set. The management of an agency cannot act one way and expect others in the agency to behave differently.

Creating a Positive Workplace Environment

Research results indicate that wrongdoing occurs less frequently when employees have positive feelings about an employer than when they feel abused, threatened, or ignored. Without a positive workplace environment, there are more opportunities for poor employee morale, which can affect an employee's attitude about committing fraud against an employer.

Employees should be empowered to help create a positive workplace environment and support the agency's values and code of conduct. They should be given the opportunity to provide input to the development and updating of the agency's code of conduct, to make certain that it is relevant, clear, and fair. Involving employees in this fashion may also effectively contribute to the oversight of the agency's code of conduct and an environment of ethical behavior.

Employees should be given the means to obtain advice internally before making decisions that appear to have significant legal or ethical implications. They should also be encouraged and given the means to communicate concerns, anonymously if preferred, about potential violations of the agency's code of conduct, without fear of retribution. Many organizations have

implemented a process for employees to report on a confidential basis any actual or suspected wrongdoing, or potential violations of the code of conduct or ethics policy. For example, some organizations use a telephone "hotline" that is directed to or monitored by an ethics officer, fraud officer, general counsel, internal audit director, or another trusted individual responsible for investigating and reporting incidents of fraud or illegal acts.

Hiring, Training and Promoting Appropriate Employees

Each employee has a unique set of values and personal code of ethics. When faced with sufficient pressure and a perceived opportunity, some employees will behave dishonestly rather than face the negative consequences of honest behavior. The threshold at which dishonest behavior starts, however, will vary among individuals. If an agency is to be successful in preventing fraud, it must have effective policies that minimize the chance of hiring or promoting individuals with low levels of honesty, especially for positions of trust.

Confirmation

Management needs to clearly articulate that all employees will be held accountable to act within the agency's code of conduct. All employees within senior management and the finance function, as well as other employees in areas that might be exposed to unethical behavior (for example, procurement and sales) should be required to sign a code of conduct statement annually, at a minimum.

Requiring periodic confirmation by employees of their responsibilities will not only reinforce the policy but may also deter individuals from committing fraud and other violations and might identify problems before they become significant. Such confirmation may include statements that the individual understands the agency's expectations, has complied with the code of conduct, and is not aware of any violations of the code of conduct other than those the individual lists in his or her response. Although people with low integrity may not hesitate to sign a false confirmation, most people will want to avoid making a false statement in writing. Honest individuals are more likely to return their confirmations and to disclose what they know (including any conflicts of interest or other personal exceptions to the code of conduct). Thorough follow-up by internal auditors or others regarding non-replies may uncover significant issues.

Discipline

The way an agency reacts to incidents of alleged or suspected fraud will send a strong deterrent message throughout the agency, helping to reduce the number of future occurrences. The following actions should be taken in response to an alleged incident of fraud:

- A thorough investigation of the incident should be conducted.
- Appropriate and consistent actions should be taken against violators.
- Relevant controls should be assessed and improved.
- Communication and training should occur to reinforce the agency's values, code of conduct, and expectations.

Expectations about the consequences of committing fraud must be clearly communicated throughout the agency. For example, a strong statement from management that dishonest actions will not be tolerated, and that violators may be terminated and referred to the appropriate authorities, clearly establishes consequences and can be a valuable deterrent to wrongdoing. If wrongdoing occurs and an employee is disciplined, it can be helpful to communicate that fact anonymously in an employee newsletter or other regular communication to employees. Seeing that other people have been disciplined for wrongdoing can be an effective deterrent, increasing the perceived likelihood of violators being caught and punished. It also can demonstrate that the agency is committed to an environment of high ethical standards and integrity.

10.5 EVALUATE ANTIFRAUD PROCESSES AND CONTROLS

Neither fraudulent financial reporting nor misappropriation of assets can occur without a perceived opportunity to commit and conceal the act. Organizations should be proactive in reducing fraud opportunities by (1) identifying and measuring fraud risks, and (2) implementing and monitoring appropriate prevent and detect internal controls and other deterrent measures.

Identifying and Measuring Fraud Risks

Management has primary responsibility for establishing and monitoring all aspects of the agency's fraud risk assessment and prevention activities. Fraud risks often are considered as part of an agency-wide risk management program, though they may be addressed separately. The fraud risk assessment process should consider the vulnerability of the agency to fraudulent activity (fraudulent financial reporting, misappropriation of assets, and corruption) and whether any of those exposures could result in a material misstatement of the financial statements or material loss to the organization. In identifying risks, organizations should consider organizational and industry-specific characteristics that influence the risk of fraud.

The nature and extent of management's risk assessment activities should be proportionate to the size of the agency and complexity of its operations. For example, the risk assessment process is likely to be less formal and less structured in smaller entities. However, management should recognize that fraud can occur in organizations of any size or type, and that almost any employee may be capable of committing fraud given the right set of circumstances. Accordingly, management should develop a heightened "fraud awareness" and an appropriate fraud risk management program, with oversight from an appropriate governing body.

Implementing and Monitoring Appropriate Internal Controls

Some risks are inherent in the environment of the agency, but most can be addressed with an appropriate system of internal control. Once a fraud risk assessment has occurred, the agency can identify the processes, controls, and other procedures that are needed to mitigate the identified risks. Effective internal control will include a well-developed control environment, an effective and secure information system, and appropriate control and monitoring activities. Because of the importance of information technology in supporting operations and the processing of transactions, management also needs to implement and maintain appropriate controls, whether automated or manual, over computer-generated information.

In particular, management should evaluate whether appropriate internal controls have been implemented in any areas management has identified as posing a higher risk of fraudulent activity, as well as controls over the agency's financial reporting process.

10.6 OTHER RESOURCES

In December 2005, the Office of the State Controller adopted a Code of Ethics that is intended to serve as a standard for Chief Financial Officers, as well as all other professionals involved in the accounting and reporting of the State's finances. This Code of Ethics establishes the standard for the minimum levels of expected behavior, and is also intended to serve as a guide for making ethical positions.

The Code of Ethics can be found at www.ncosc.net/about/professional_ethics.html.

The North Carolina Office of the State Auditor has established a fraud hotline. Those who suspect fraud in their organization are encouraged to report it. All allegations of improper activities remain confidential and state law provides protections from retaliation or discrimination for employees who report improper or illegal activities.

The State Auditor's hotline number is: **1-800-730-TIPS**.

To obtain more information on fraud and implementing antifraud programs and controls, please go to the following Web sites where additional materials, guidance, and tools can be found:

American Institute of Certified Public Accountants - http://www.aicpa.org/
Association of Certified Fraud Examiners - http://www.acfe.com/
Government Accounting Standards Board - http://www.gasb.org/
Government Finance Officers Association - http://www.gfoa.org/
Information Systems Audit and Control Association - http://www.isaca.org/
The Institute of Internal Auditors - http://www.theiia.org
Institute of Management Accountants - http://www.imanet.org/
National Association of Corporate Directors - http://www.nacdonline.org/
National Association of State Auditors, Comptrollers, and Treasurers - http://www.nasact.org/
North Carolina Office of the State Auditor - http://www.ncauditor.net/
Society for Human Resource Management - http://www.shrm.org/
The U.S. Government Accountability Office - http://www.gao.gov
The Office of Management and Budget - http://www.whitehouse.gov/omb

11. CONCLUSION

11.1 EAGLE PROGRAM

Effective internal controls are the foundation for managing risk and creating a safe and sound operating environment. The EAGLE Program was created to establish adequate internal control and to increase fiscal accountability within State government.

Under the EAGLE Program, each agency is required to perform an annual assessment of internal control. By performing this assessment, agencies can identify risks and compensating controls that reduce the possibility of material misstatements, misappropriation of assets and noncompliance with laws and regulations. The assessment will also indicate opportunities for increased efficiency and control effectiveness in agency processes and operations.

11.2 CONTACT INFORMATION

For further information on the EAGLE Program or for assistance, agencies may use the following resources:

EAGLE Program Website through OSC: http://www.osc.nc.gov/eagle/

EAGLE Support line:
Call (919) **707-0795**
Email OSC.EagleSupport@lists.osc.nc.gov

APPENDICES

Note: The Financial templates linked in the Appendices section are examples of how to complete the templates. The Compliance templates are blank templates; please refer to the compliance case study located on the EAGLE Site.

APPENDIX 4.1A – FINANCIAL MATERIALITY & ACCOUNT RISK

Agency ABC

Legend	
	Auto Calculating Field
	User Entry Field
	Copy from DSS

Materiality Threshold	
1%	Low=1
1% - 5%	Moderate=2
5%	High=3

Prepared by:	T. Smith
Reviewed by:	J. Doe

Materiality & Account Risk Assessment – Consolidated Fund

Materiality				Account Risk Assessment						
Account Caption	Account Balance	Materiality Percentage per Materiality Guidance		Materiality	Size and Composition	Transaction Volume	Transaction Complexity	Subjectivity / Estimation	Inherent Risk	Total Score	Stop or Continue to Process Risk
Balance Sheet Assets	Use Prior Year Financial Statements	% Total Assets & Other Debits	(Proprietary only) % Total Assets less Total Capital Assets								
. Cash and cash equivalents	17,671.00	0.55%		Low	1	1	1	1	2	6	Stop
. Pooled cash	1,407,624.00	43.67%		High	3	3	1	1	3	11	**Continue**
. Accounts receivable	105,746.00	3.28%		Moderate	2	1	1	2	2	8	Stop
. Intergovernmental receivables	778,407.00	24.15%		High	3	1	1	1	2	8	Stop
. Interest receivable	154,683.00	4.80%		Moderate	2	1	1	1	1	6	Stop
Due from other funds	612,954.00	19.02%		High	3	1	1	1	1	7	Stop
Inventories	33,655.00	1.04%		Moderate	2	1	1	1	2	7	Stop
Notes receivable	49,511.00	1.54%		Moderate	2	1	1	1	1	6	Stop
Amount available and to be provided	63,061.00	1.96%		Moderate	2	1	1	2	2	8	Stop
Liabilities											
. Accounts payable	201,889.00	6.26%		High	3	2	2	2	2	11	**Continue**
. Accrued payroll	31,776.00	0.99%		Low	1	2	1	2	1	7	Stop
. Intergovernmental payables	825,614.00	25.61%		High	3	1	1	2	1	8	Stop
Due to other funds	154,419.00	4.79%		Moderate	2	1	1	1	1	6	Stop
Deferred revenue	93,293.00	2.89%		Moderate	2	1	1	3	1	8	Stop
Funds held for others	7,902.00	0.25%		Low	1	1	2	1	2	7	Stop
Accrued vacation leave	63,061.00	1.96%		Moderate	2	2	1	2	1	8	Stop

Note: Completed portion for example purposes only.

Low	Total Score of 8 or less.
Moderate	Total Score of less than 12 but greater than 8.
High	Total Score of 12 or greater.

APPENDIX 4.1A – FINANCIAL PROCESS RISK ASSESSMENT

Appendix 4.1 A

Risk Assessment Template – Process Risk

EAGLE Program
Agency ABC
Fund Name
Process Risk Assessment
6/30/20XX

Prepared by:	T. Smith
Reviewed by:	J. Doe

From Account Risk Assessment										
Account Caption	Account Risk Rating (Moderate or High)	Significant Processes	Size and Composition	Susceptibility Due to Error / Fraud	Complexity of Transactions	Similarity of Transactions	IT Dependency / Manual Intervention	Degree of Subjectivity / Estimation	Total Score	Stop or Continue to Location Risk or to Narrative At least one process must be documented for each account.
Accounts Payable/Expenditures	**High**	New Vendor Setup	3	3	2	2	3	2	15	**Continue**
		Purchasing	3	2	2	2	1	1	11	**Continue**
		Receiving	2	2	1	2	3	2	12	**Continue**
		Processing Invoices	3	3	2	3	2	2	15	**Continue**
		Payments	3	3	2	3	2	2	15	**Continue**
		Update to G/L/Accrual Process	3	2	2	2	1	2	12	**Continue**
		AP Applications and Data Access	3	3	2	2	2	1	13	**Continue**

Note: Completed portion for example purposes only.

To rate each process above enter a 1 for Low, 2 for Moderate or 3 for High. The Process Risk Assessment should be completed for all account captions with a total score of Moderate or High on the Account Risk Assessment.

After completing the above Process Risk Assessment, if a significant process is High or Moderate risk and performed at more than one location, you must complete the

Low	Total Score of 10 or less.
Moderate	Total Score of less than 15 but greater than 10.
High	Total Score of 15 or greater.

APPENDIX 4.1A – FINANCIAL LOCATION RISK ASSESSMENT

Legend	
	Auto Calculating Field
	User Entry Field
	Copy from Process Risk

EAGLE Program
College Name

Location Risk Assessment
6/30/20XX

Prepared by:	
Reviewed by:	

From Process Risk Assessment											
Account	Significant Process	Process Risk Rating (Moderate or High)	Locations	Prior Year Issues	IT Environment	Complexity of Business and Accounting Transactions	Changes in Business or Accounting Transactions	Quantitative Significance	Total Score	Stop or Continue to Narrative
Cash & Cash Equivalents; Restricted Cash & Cash Equivalents	*Cash Receipts - Manual*	*High*	Cashiers Office	1	3	1	1	3	*9*	Stop
			Bookstore	1	3	1	1	2	*8*	Stop
			Library	1	3	1	1	1	*7*	Stop
			Cont. Ed. Programs	3	3	1	1	2	*10*	Stop
									0	
									0	

To rate each location above enter a 1 for Low, 2 for Moderate or 3 for High.

If a significant process is High risk and performed at more than one location, you must complete the Location Risk Assessment template. Location risk helps management to understand which locations represent the highest risk for each financial statement account and consequently require the most effort to document and test. If a significant process is not performed at more than one location, the Location Risk Assessment template is not applicable.

Low	Total Score of 8 or less.
Moderate	Total Score of less than 12 but greater than 8.
High	Total Score of 12 or greater.

APPENDIX 4.1B – PROGRAM/GRANT MATERIALITY AND RISK ASSESSMENT

EAGLE Program

Agency Name

Schedule of Expenditures of Federal Awards

Program/Grant Risk Assessment

June 30, 20XX

Prepared by:	
Reviewed by:	

Legend	
	Auto Calculating Field
	User Entry Field
	Copy from SEFA

Materiality Threshold	
≤ 10%	Low=1
10%> <50%	Moderate=2
≥ 50%	High=3

	Materiality			Program/Grant Risk Assessment				
Federal CFDA Number	CFDA Program Title	Total Federal Awards Expended as of 20XX	Materiality	Size and Composition	Program/Grant Complexity	Inherent Risk	Total Score	Stop or Continue to Requirement Risk
							0	
							0	
							0	
	Total	$ -						

To rate each program/grant above enter a 1 for Low, 2 for Moderate or 3 for High.

Moderate and High risk programs/grants will move forward to the Requirement Risk Assessment.

Low	Total Score of 4 or less.
Moderate	Total Score of less than 7 but greater than 4.
High	Total Score of 7 or greater.

APPENDIX 4.1B – PROGRAM/GRANT REQUIREMENT RISK ASSESSMENT

EAGLE Program
Agency Name
Schedule of Expenditures of Federal Awards
Requirement Risk Assessment
June 30, 20XX

Legend	
	Auto Calculating Field
	User Entry Field
	Copy from Materiality & Program/Grant Risk Assessment
	Refer to Tab "Circular A-133".

Prepared by:	
Reviewed by:	

From Materiality & Program/Grant Risk Assessment										
Federal CFDA Number	CFDA Program Title	Program/Grant Risk Rating (High or Moderate)	Types of Compliance Requirements	A-133 Requirement (Yes or No)	Stop or Continue	Size and Composition	Complexity of Requirement	Susceptibility Due to Error / Fraud	Total Score	Stop or Continue to Compliance Narrative
			Activities Allowed or Unallowed	<Select Answer>					0	Stop
			Allowable Costs/Cost Principles	<Select Answer>					0	Stop
			Cash Management	<Select Answer>					0	Stop
			Davis-Bacon Act	<Select Answer>					0	Stop
			Eligibility	<Select Answer>					0	Stop
			Equipment and Real Property Management	<Select Answer>					0	Stop
			Matching, Level of Effort, Earmarking	<Select Answer>					0	Stop
			Period of Availability of Federal Funds	<Select Answer>					0	Stop
			Procurement and Suspension and Debarment	<Select Answer>					0	Stop
			Program Income	<Select Answer>					0	Stop
			Real Property Acquisition/Relocation Assistance	<Select Answer>					0	Stop
			Reporting	<Select Answer>					0	Stop
			Subrecipient Monitoring	<Select Answer>					0	Stop
			Special Tests and Provisions	<Select Answer>					0	Stop
			Special Tests and Provisions (ARRA)	<Select Answer>					0	Stop

To rate each program/grant above, enter a 1 for Low, 2 for Moderate or 3 for High. The Requirement Risk Assessment should be completed for all programs/grants with a total score of High or Moderate on the Materiality & Program/Grant Risk Assessment.

Low	Total Score of 5 or less.
Moderate	Total Score of 6.
High	Total Score of 7 or greater.

APPENDIX 4.2A
FINANCIAL ASSESSMENT RISK CRITERIA GUIDANCE

Document:	**Account Risk Assessment Guidance**		**Prepared by: T. Smith**
Entity:	*Agency Name*		**Reviewed by: J. Doe**

	High (Points – 3)	**Moderate (Points – 2)**	**Low (Points – 1)**
Size and Composition *Automatically populates in Risk Assessment template.*	Account balance greater than or equal to High materiality.	Account balance less than High materiality but greater than Low materiality.	Account balance less than or equal to Low materiality.
Transaction Volume *Customize for your agency per fund (## of transactions).*	Multiple transactions per day.	More than ## transactions per year but less frequent than one transaction per day.	Less than ## transactions per year.
Transaction Complexity	Transactions are complex in nature (i.e., complex calculations, requiring significant financial disclosures, complex accounting guidance associated with account, etc.).	Majority of the transactions are non-complex. However, some transactions require additional attention due to their complexity.	Transactions are routine in nature.
Subjectivity and Estimation	75% of the account balance is based on subjectivity or estimates.	Greater than 10% but less than 75% of the account balance is based on subjectivity or estimates.	Less than 10% of the account balance is based on subjectivity or estimates.
Inherent Risk *Also, includes any other risk factors not captured above.*	High probability that errors or fraud would impact the account; History of reoccurring or recent audit findings or material adjustments; Recent fraudulent activity.	Reasonably probable that errors or fraud would impact the account; History of past audit findings or immaterial adjustments; Past fraudulent activity.	Low probability of errors or fraud; No history of audit findings, adjustments or fraud.
Total Score	Total Score of 12 or greater.	Total Score less than 12 but greater than 8.	Total Score of 8 or less.

APPENDIX 4.2A
FINANCIAL ASSESSMENT RISK CRITERIA GUIDANCE

Document:	Process Risk Assessment Guidance	Prepared by: T. Smith
Entity:	*Agency Name*	Reviewed by: J. Doe

	High (Points – 3)	Moderate (Points – 2)	Low (Points – 1)
Size and Composition	Process impacts the account balance by greater than or equal to 30% of account balance.	Process impacts the account balance by less than 30% but greater than 10% of account balance.	Process impacts the account balance by less than or equal to 10% of account balance.
Susceptibility Due to Error / Fraud	High probability that errors or fraud could impact the process; History of reoccurring or recent audit findings and/or material adjustments impacting the process; Recent fraudulent activity in the process.	Reasonably probable that errors or fraud could impact the process; History of past audit findings and/or immaterial adjustments impacting the process; Past fraudulent activity in the process.	Low probability of errors or fraud; No history of audit findings or fraud impacting the process.
Complexity of Transactions	Business and accounting transactions are highly complex.	Business and accounting transactions are moderately complex.	Business and accounting transactions are not complex.
Similarity of Transactions	Less than 25% of the transactions are similar in nature.	Between 25% and 75% of the transactions are similar in nature.	At least 75% of the transactions are similar in nature.
IT Dependency / Manual Intervention	Highly manual complex processes. IT infrastructure is an older version with many manual interfaces.	Moderately automated process.	Highly automated process.
Degree of Subjectivity / Estimation	75% of the account balance impacted by the process is based on subjectivity or estimates.	Greater than 10% but less than 75% of the account balance impacted by the process is based on subjectivity or estimates.	Less than 10% of the account balance impacted by the process is based on subjectivity or estimates.
Total Score	Total Score of 15 or greater.	Total Score less than 15 but greater than 10.	Total Score of 10 or less.

APPENDIX 4. 2A
FINANCIAL ASSESSMENT RISK CRITERIA GUIDANCE

Document:	**Location Risk Assessment Guidance**		**Prepared by: T. Smith**
Entity:	*Agency Name*		**Reviewed by: J. Doe**

	High (Points - 3)	**Moderate (Points - 2)**	**Low (Points - 1)**
Prior Year Issues	Significant prior year errors or issues resulting in audit findings and/or material adjustments or restatements. Prior year issues due to control failure.	Prior year errors or issues that did not result in audit findings and/or material adjustments or restatements. Prior year issues due to control failure.	No prior year issues.
IT Environment	Highly manual complex processes. IT infrastructure is from unknown vendor and/or version is more than 10 years old.	Moderately automated processes. Leverage some automated controls. IT infrastructure is from reputable vendor and version is between 5 and 10 years old.	Highly automated processes. Leverage automated controls. IT infrastructure is from reputable vendor and version is less than 5 year old.
Complexity of Business and Accounting Transactions	Business and accounting transactions are complex.	Business and accounting transactions are moderately complex.	Business and accounting transactions are not complex.
Changes in Business or Accounting Transactions	Rapid growth in business. Developing or offering new products/services. Significant change in the business model.	Moderate growth in business. Developing or offering some new products/services.	Maintain consistent products/services from prior years. Consistent business model.
Quantitative Significance	Account balances are significant to more than 5% of consolidated financial statements.	Account balances are significant to between 1% and 5% of consolidated financial statements.	Account balances are significant to less than 1% of consolidated financial statements.
Total Score	Total Score of 12 or greater.	Total Score less than 12 but greater than 8.	Total Score of 8 or less.

APPENDIX 4. 2B
COMPLIANCE RISK ASSESSMENT CRITERIA GUIDANCE

Document:	**Materiality & Program/Grant Risk Assessment Guidance**		**Prepared by:**
Entity:	*Agency Name*		**Reviewed by:**

	High (Points – 3)	**Moderate (Points – 2)**	**Low (Points – 1)**
Size and Composition *Automatically populates in Risk Assessment template.*	Program/grant expenditures greater than or equal to High materiality.	Program/grant expenditures less than High materiality but greater than Low materiality.	Program/grant expenditures less than or equal to Low materiality.
Program/Grant Complexity	New or complex program/compliance requirements; Less experienced or new compliance personnel.	Majority of the program/compliance requirements are non-complex. However, some requirements involve additional attention due to their complexity.	Non-complex compliance requirements. Highly experienced and knowledgeable compliance personnel.
Inherent Risk *Also, includes any other risk factors not captured above.*	High probability that errors or fraud could occur; History of recurring or recent audit findings or recent fraudulent activity.	Reasonably probable that errors or fraud could occur; History of past audit findings or past fraudulent activity.	Low probability of errors or fraud; No history of audit findings or fraud in previous 5 fiscal years.
Total Score	Total Score of 7 or greater.	Total Score of less than 7 but greater than 4.	Total Score of 4 or less.

APPENDIX 4. 2B
COMPLIANCE RISK ASSESSMENT CRITERIA GUIDANCE

Document:	**Requirement Risk Guidance**		**Prepared by:**
Entity:	*Agency Name*		**Reviewed by:**

	High (Points – 3)	**Moderate (Points – 2)**	**Low (Points – 1)**
Size and Composition	30% or more of grant expenditures are applicable to this compliance requirement.	Greater than 10% but less than 30% of grant expenditures are applicable to this compliance requirement.	Less than 10% of grant expenditures are applicable to this compliance requirement.
Complexity of Requirement	Compliance requirement is new and/or highly complex.	Compliance requirement is non-complex. However, some aspects of the requirements involve additional attention due to the complexity.	Compliance requirement is not complex.
Susceptibility Due to Error / Fraud	High probability that errors or fraud could occur; History of recurring or recent audit findings or recent fraudulent activity.	Reasonably probable that errors or fraud could occur; History of past audit findings or past fraudulent activity.	Low probability of errors or fraud; No history of audit findings or fraud in previous 5 fiscal years.

APPENDIX 4.2C – ASSERTION RISK GUIDANCE

APPENDIX 4.2C1

EAGLE Program

Financial Statement Assertion Guidance

June 30, 20XX

Questions to consider when identifying and documenting processes and controls:	Financial Statement Assertions				
	Existence or Occurrence	**Completeness**	**Rights and Obligations**	**Valuation or Allocation**	**Presentation and Disclosure**
Cash ***Segregation of Duties Controls***					
Are responsibilities for cash collections segregated from those for preparing the deposit?	X	X		X	
Are responsibilities for collections and deposit preparation segregated from those for recording general ledger entries?		X			
Are responsibilities for cash receipting segregated from those for cash disbursing?	X	X			
Are all reconciliations and investigations of unusual reconciling items reviewed and approved on a monthly basis by an official who is not responsible for receipts and disbursements, including recording evidence of the review and approval by signing the reconciliation?	X	X		X	
Procedural Controls ***General***					
Do procedures exist to ensure that collections and disbursements are recorded accurately and promptly?	X	X		X	X
Do controls exist over the collection, timely deposit, and recording of collections in the accounting records in each collection location?	X	X			

Receipts					
Is a restrictive endorsement placed on each incoming check upon receipt?	X				
Are receipts controlled by cash register, pre-numbered receipts, or other equivalent means if payments are made in person (over the counter)?	X	X			
Are receipts accounted for and balanced to collections on a daily basis?	X	X			
Are undeposited cash receipts protected?	X	X			
Deposits					
Are total receipts reconciled to the validated deposit slip?	X	X			
Are receipts deposited daily as required by Daily Deposit Act?	X		X		
Cash Disbursements					
Are controls in place for the use of warrant or check-signing machines and electronic signatures?	X	X			
Are two signatures required on warrants or checks over a stated amount?	X				
Are controls maintained over the supply of unused and voided warrants or checks?	X	X			
Bank Reconciliations					
Does management review and approve bank reconciliations on a monthly basis?		X			
Are procedures in place to follow up on outstanding items?	X	X			
Are timely corrective actions taken in cash discrepancies?				X	

APPENDIX 4.2C2

EAGLE Program

Financial Statement Assertion Guidance

June 30, 20XX

Questions to consider when identifying and documenting processes and controls:	Financial Statement Assertions				
	Existence or Occurrence	**Completeness**	**Rights and Obligations**	**Valuation or Allocation**	**Presentation and Disclosure**
Investments					
Segregation of Duties Controls					
Are responsibilities for initiating investment transactions segregated from those for approving investments?	X		X		
Are responsibilities for initiating, evaluating, and approving transactions segregated from those for detail accounting, general ledger, and other related functions?	X	X		X	
Are responsibilities for monitoring investment market values and performance segregated from those for investment acquisition?	X			X	
Are responsibilities for maintaining detail accounting records segregated from those for general ledger entries?	X	X		X	
Are custodial responsibilities for securities or other documents evidencing ownership or other rights assigned to an official who has no accounting duties and no authorization to purchase, exchange, or sell investments?	X		X	X	
Procedural Controls					
Approval					
Are procedures adequate to ensure that only investments that are permitted by law or policies are acquired?	X				X
Do approval procedures include formal establishment and annual review of investment policies and guidelines?	X				X

Are there formal procedures governing the level and nature of approvals required to purchase, exchange or sell an investment?	X		X	X	
Is the investment program integrated with the cash management program and expenditure requirements?	X	X		X	
Is the performance of the investment portfolio periodically evaluated by persons independent of investment portfolio management activities?	X			X	
Are competitive bids sought for certificate of deposit purchases?	X			X	
Custodian					
Are all securities and legal documents or agreements, evidencing ownership or other rights, kept in a safe deposit box, safe, or vault?	X		X		
Do custodial procedure include registering all securities in the name of the governmental unit?	X		X		X
Do custodial procedures include bonding of individuals with access to securities?	X				
Are securities periodically inspected or confirmed monthly from custodial agents?	X	X		X	X
Detail Accounting					
Is an accounting/custodian record maintained for each investment, including the CUSIP or SEDOL number, description, date purchased, interest rate, maturity date, Face amount, premium or discount, and proceeds?	X	X		X	X
Are there controls to ensure investment transactions are recorded on a timely basis?		X		X	
Are there procedures to ensure transactions arising from investments are properly processed, including income and amortization (13th month fair value) entries?	X	X		X	X
Do detail accounting procedures include a periodic comparison between income received and the amount specified by the terms of the investment?	X	X		X	

Are there controls to ensure that investment earnings are credited to the fund from which resources were provided for the investment?			X	X	X
General Ledger					
Are procedures in place to reconcile the detail accounting records (custodian statement) with the general ledger balances?	X	X		X	X
Do procedures include monthly verification of all investments and collateral to the custodian statement?		X		X	X
Do procedures include a review and approval of all investment reconciliations by an official not responsible for receipts and disbursements?	X	X			
Do the reconciliation procedures include an investigation of unusual reconciling items by an official not responsible for receipts and disbursements?	X	X		X	
Are the reconciliations prepared timely and signed by an official not responsible for receipts and disbursements?	X	X			

APPENDIX 4.2C3

EAGLE Program

Financial Statement Assertion Guidance

June 30, 20XX

Questions to consider when identifying and documenting processes and controls:	**Financial Statement Assertions**				
	Existence or Occurrence	**Completeness**	**Rights and Obligations**	**Valuation or Allocation**	**Presentation and Disclosure**
Capital Assets ***Segregation of Duties Controls***					
Are responsibilities for initiating, evaluating, and approving capital expenditures, leases, and maintenance or repair projects segregated from those for project accounting, property records, and general ledger functions?	X	X			

Are responsibilities for initiating capital asset transactions segregated from those for final approvals that commit government resources?	X	X		X	
Are responsibilities for the project accounting and property records functions segregated from the general ledger function?	X	X		X	
Are responsibilities for the periodic physical inventories of capital assets assigned to responsible officials who have no custodial or record keeping responsibilities?	X	X			
Procedural Controls					
General					
Do physical safeguards over assets exist?	X				
Are furniture and equipment properly assigned a fixed asset number and tagged as a means of positive identification?	X		X		
Are fixed asset system records and capital assets subsidiary accounts periodically reconciled with the general ledger control accounts?	X	X		X	X
Are the beginning balances, additions, disposals and ending balances reflected in the note disclosures reconciled to the fixed asset system?		X		X	X
Additions					
Are records maintained in the fixed asset system for all significant self-constructed, donated, purchased, or leased assets?	X		X		
Do procedures exist to identify supplies and materials expenses that are to be capitalized?				X	X
Are procedures in place at year-end to review the construction in progress account for amounts that should be reclassified as depreciable assets?	X	X			X
Deletions					
Do procedures exist for authorizing, approving, and documenting sales or other dispositions of capital assets?	X	X			

Are the accounting records adjusted promptly-both the asset and related allowance for depreciation-when items of plant and equipment are retired, sold, or transferred?	X		X	X	X
Depreciation					
Do procedures exist to govern depreciation methods and practices?				X	X
Inventory					
Is a physical inventory of capitalized assets taken at least annually?	X	X	X		
Are differences between records and physical counts investigated and are the records adjusted to reflect actual counts?	X	X			

APPENDIX 4.2C4

EAGLE Program

Financial Statement Assertion Guidance

June 30, 20XX

Questions to consider when identifying and documenting processes and controls:	**Financial Statement Assertions**				
	Existence or Occurrence	**Completeness**	**Rights and Obligations**	**Valuation or Allocation**	**Presentation and Disclosure**
Revenue Accounts ***Segregation of Duties Controls***					
Are billing responsibilities segregated from collection activities?	X				
Are billing and collection activities segregated from the accounting records maintenance function?	X	X		X	
Are responsibilities for maintaining detail accounts receivable records segregated from those for general ledger entries?	X	X			
Are responsibilities for reconciling and investigating reconciling items segregated from those for posting detail accounts receivable records?	X	X			

Procedural Controls					
General					
Are customer databases and usage records accurately maintained to ensure that amounts due are billed correctly?	X	X			
Are invoices billed in a timely fashion?		X			
Are rates for taxes, fees, licenses, fines, and other services periodically reviewed and approved?				X	
Are controls in place to ensure timely payment of amounts due?		X		X	
Is an aging schedule prepared monthly and reviewed by management?	X	X			
Are all non-cash credits, such as credit memos, allowances, and bad debts properly authorized?	X			X	
Taxes					
Are tax returns reviewed for mathematical accuracy?				X	
Are claims for tax refunds reviewed and approved separately?	X			X	
Collections					
Are amounts collected on behalf of other agencies identified and remitted on a timely basis?				X	X
Are taxes and fees collected by another agency monitored to assure timely receipt and are amounts received subjected to reviews for reasonableness?		X		X	
Are accounts receivable records maintained and used as a basis for collections?		X		X	
Are procedures in place to follow up on delinquent accounts?		X			
Are all legal remedies followed to collect write-offs or uncollectible accounts with the Attorney General?				X	

Allowances / Write-Offs (Accounts Receivable)					
Has an allowance account been established for doubtful accounts to reflect the amount of the agency's receivables that management estimates will be uncollectible?		X		X	X
Are accounts written off the agency's financial accounts when all collection procedures have been exhausted without success and reasons adequately documented?	X			X	
Do write-offs or adjustments have proper authorization?	X			X	

APPENDIX 4.2C5

EAGLE Program
Financial Statement Assertion Guidance
June 30, 20XX

Questions to consider when identifying and documenting processes and controls:	**Financial Statement Assertions**				
	Existence or Occurrence	**Completeness**	**Rights and Obligations**	**Valuation or Allocation**	**Presentation and Disclosure**
Procurements (Expenditure Accounts) *Segregation of Duties Controls*					
Are responsibilities for the requisitioning, purchasing, and receiving functions segregated from the invoice processing, and general ledger functions?	X	X			
Are responsibilities for the requisitioning and purchasing functions segregated from the receiving functions?	X	X			
Are responsibilities for the invoice processing function segregated from the general ledger function?	X	X		X	

Procedural Controls					
Purchasing					
Are purchases of goods and services initiated by properly authorized requisitions bearing the approval of officials designated to authorize requisitions?	X				
Do approval procedures exist for purchase order and contract issuance?	X				
Are competitive bidding procedures used?				X	
Are an adequate number of price quotations obtained before placing orders not subject to competitive bidding?				X	
Is splitting orders to avoid higher levels of approval prohibited?	X			X	
Are price lists and other appropriate records of price quotations maintained by the purchasing department?				X	
Is a record of suppliers who have not met quality or other performance standards by the purchasing department maintained?	X	X			
Are procedures instituted to identify, before order entry, costs and expenditures not allowable under grant (federal/state) programs?				X	
If construction contracts are to be awarded, are bid and performance bonds considered?	X			X	
Does predetermining selection criteria exist for awarding personal service or construction contracts and is adequate documentation of the award process required?				X	
Are changes to contracts or purchase orders subjected to the same controls and approvals as the original agreement?				X	
Receiving					
Are steps taken to ensure that goods received are accurately counted and examined to see that they meet quality standards?	X			X	
Does the receiving department send copies of receiving reports directly to purchasing and accounting?	X	X		X	

Are requests for progress payments to contractors formally approved by a contract administrator/officer after project inspection?	X	X		X	
If a receiving department is not used, do adequate procedures exist to ensure that goods for which payment is made have been received and are verified by someone other than the individual approving payment that goods have been received and meet quality standards?	X	X		X	
Are P-card purchases reconciled monthly by someone other than the card holder?	X	X			
Invoice Processing					
Are invoice quantities, prices, and terms compared with those indicated on the purchase order?		X		X	
Are invoice quantities compared with those indicated on the receiving reports?		X		X	
Are all invoices received from vendors in a central location, such as the accounting department?		X			
Are employee travel requests approved before the expenditure is incurred?	X				
Do procedures exist for submission and approval of reimbursement to employees for travel and other expenses?	X			X	
Are invoices (vouchers) properly approved after review for accuracy and completeness of supporting documents?	X	X		X	
Are payments made only on the basis of original invoices?	X			X	
Are there steps in the processing procedures to prevent or detect duplicate payments, such as stamping invoices paid?	X				
Are payments made as close to the discount date as possible and are tax exemptions claimed?				X	
Are subrecipient invoices subjected to a desk review by a contract/project administrator before payment approval?	X			X	

General Ledger (Liabilities)					
Are procedures in place to determine expenditures for goods and services that are payable at year-end?	X	X	X		X
Are accruals and adjusting entries and journal entries reviewed for reasonableness and approved by someone other than the preparer?	X	X	X	X	X

APPENDIX 4.2C6

EAGLE Program

Financial Statement Assertion Guidance

June 30, 20XX

Questions to consider when identifying and documenting processes and controls:	**Financial Statement Assertions**				
	Existence or Occurrence	**Completeness**	**Rights and Obligations**	**Valuation or Allocation**	**Presentation and Disclosure**
Payroll Accounts ***Segregation of Duties Controls***					
Are responsibilities for supervision and timekeeping functions segregated from personnel, payroll processing, disbursement, and general ledger functions?	X	X			
Is the payroll register reconciled to general ledger payroll accounts regularly by employees independent of all other payroll transaction processing activities?	X	X		X	
Procedural Controls ***Personnel***					
Are all changes in employment (additions and terminations), salary and wage rates, and payroll deductions properly authorized, approved, and documented?	X	X		X	
Are notices of additions, separations, and changes in salaries, wages, and deductions promptly reported to Human Resources?		X		X	

Supervision/Timekeeping					
Are hours worked, overtime hours, and other special benefits reviewed and approved by the employee's supervisor?	X	X		X	
Do procedures exist for authorizing, approving, and recording vacations, holidays, and sick leave and is compensatory time controlled and approved?	X			X	X
Payroll Processing					
Is access to the BEACON master payroll file limited to employees who are authorized to make changes?	X			X	
Are completed payroll registers reviewed and approved before disbursements are made?	X	X		X	
Is the payroll (examination of authorizations for changes noted on reconciliations) reviewed by an employee not involved in its preparation?	X	X		X	
Are comparisons of gross pay for current to prior period payrolls reviewed for reasonableness by someone outside of Human Resources?	X	X		X	
Are procedures in place to reconcile BEACON to NCAS and CMCS?		X		X	
General Ledger (includes Liabilities)					
Do adequate account coding procedures exist for classification of employee compensation and benefit costs so that such costs are recorded in the proper general ledger account?					X
Are individual employee leave records reconciled, at least annually, to appropriate records maintained for accumulated employee benefits (vacation, sick leave, etc.)?	X		X	X	X
Are accrued liabilities for unpaid employee compensation and benefit costs and compensated absences properly recorded or disclosed?		X	X	X	X

APPENDIX 4.2D
COMPLIANCE INTERNAL CONTROLS GUIDANCE

APPENDIX 4.2D1

ACTIVITIES ALLOWED OR UNALLOWED AND ALLOWABLE COSTS/COST PRINCIPLES

Description of Compliance Requirement

The specific requirements for activities allowed or unallowed are unique to each Federal program and are found in the laws, regulations, and the provisions of contract or grant agreements pertaining to the program. This type of compliance requirement specifies the activities and costs that can or cannot be funded under a specific program. For details (matrix) on Allowable Costs/Cost Principles, refer to A-133 Part 3 Allowable Costs/Cost Principles.

Control Objectives

To provide reasonable assurance that Federal awards are expended only for allowable activities and that the costs of goods and services charged to Federal awards are allowable and in accordance with the applicable cost principles.

Controls:

- Accountability provided for charges and costs between Federal and non-Federal activities.
- Process in place for timely updating of procedures for changes in activities allowed and cost
- Computations checked for accuracy.
- Supporting documentation compared to list of allowable and unallowable expenditures.
- Adjustments to unallowable costs made where appropriate and follow-up action taken to
- Adequate segregation of duties in review and authorization of costs.
- Accountability for authorization is fixed in an individual who is knowledgeable of the requirements for determining activities allowed and allowable costs.
- Reports, such as a comparison of budget to actual provided to appropriate management for review
- Management reviews supporting documentation of allowable cost information.
- Comparisons made with budget and expectations of allowable costs (Analytic reviews).

APPENDIX 4.2D2 CASH MANAGEMENT

Description of Compliance Requirement

When entities are funded on a reimbursement basis, program costs must be paid for by entity funds before reimbursement is requested from the Federal Government. When funds are advanced, recipients must follow procedures to minimize the time elapsing between the transfer of funds from the U.S. Treasury and disbursement.

Control Objectives

To provide reasonable assurance that the draw down of Federal cash is only for immediate needs. States comply with applicable Treasury agreements, and recipients limit payments to subrecipients to immediate cash needs.

Controls:

- Management has identified programs that receive cash advances and is aware of cash management requirements.
- Cash flow statements by program are prepared to determine essential cash flow needs.
- Accounting system is capable of scheduling payments for accounts payable and requests for funds from Treasury to avoid time lapse between draw down of funds and actual disbursements of funds.
- Appropriate level of supervisory review of cash management activities.
- Written policy that provides:
  - Procedures for requesting cash advances as close as is administratively possible to actual cash outlays;
  - Monitoring of cash management activities;
  - Repayment of excess interest earnings where required.
- For State programs subject to a Treasury-State agreement, a written policy exists which
  - Programs covered by the agreement;
  - Methods of funding to be used;
  - Method used to calculate interest; and
- Variance reporting of expected versus actual cash disbursements of Federal awards and drawdowns of Federal Funds.
- Subrecipients' requests for Federal funds are evaluated.
- Review of compliance with Treasury-State agreements.

APPENDIX 4.2D3 DAVIS-BACON ACT

Description of Compliance Requirement

Non-federal entities shall include in their construction contracts subject to the Davis-Bacon Act a requirement that the contractor or subcontractor comply with the requirements of the Davis-Bacon Act and the DOL regulations. This includes a requirement for the contractor or subcontractor to submit to the non-Federal entity weekly, for each week in which any contract work is performed, a copy of the payroll and a statement of compliance (certified payrolls).

Davis-Bacon Act only applies as required by the Act itself, the Department of Labor's (DOL) government wide implementation of the Davis-Bacon Act, ARRA or by Federal program legislation, all laborers and mechanics employed by contractors and subcontractors to work on construction contracts in excess of $2000 financed by Federal funds must be paid wages not less than those established for the locality of the project (prevailing wage rates) by DOL.

Control Objectives

To provide reasonable assurance that contractors and subcontractors were properly notified of the Davis-Bacon Act requirements and the required certified payrolls were submitted to the non-Federal entity.

Controls:

- Contractors informed in the procurement documents of the requirements for prevailing wage rates.
- Contractors and subcontractors are required by contract to submit certifications and copies of payrolls.
- Contractors' and subcontractors' payrolls monitored to ensure certified payrolls are submitted.
- Reports provide sufficient information to determine if requirements are being met.
- Management reviews to ensure that contractors and subcontractors are properly notified of the Davis-Bacon Act requirements.
- Management reviews to ensure that certified payrolls are properly received.

APPENDIX 4.2D4 ELIGIBILITY

Description of Compliance Requirement

The specific requirements for eligibility are unique to each Federal program and are found in the laws, regulations, and the provisions of contract or grant agreements pertaining to the program. This compliance requirement specifies the criteria for determining the individuals, groups of individuals (including area of service delivery), or subrecipients that can participate in the program and the amounts for which they qualify.

Control Objectives

To provide reasonable assurance that only eligible individuals and organizations receive assistance under Federal award programs, that subawards are made only to eligible subrecipients, and that amounts provided to or on behalf of eligible individuals or groups of individuals were calculated in accordance with program requirements.

Controls:

- Conflict-of-interest statements are maintained for individuals who determine and review eligibility.
- Written policies provide direction for making and documenting eligibility determinations.
- Procedures to calculate eligibility amounts consistent with program requirements.
- Authorized signatures (manual or electronic) on eligibility documents periodically reviewed.
- Adequate safeguards in place to ensure access to eligibility records (manual or electronic) limited to appropriate persons.
- Manual criteria checklists or automated process used in making eligibility determinations.
- Process for periodic eligibility re-determinations in accordance with program requirements.
- Verification of accuracy of information used in eligibility determinations.
- Procedures to ensure the accuracy and completeness of data used to determine eligibility requirements.
- Process in place to ensure benefits were discontinued when eligibility requirements no longer met or period of eligibility expired.
- Processing of eligibility information subject to edit checks and balancing procedures.
- Documentation of eligibility determinations in accordance with program requirements.
- Periodic analytical reviews of eligibility determinations performed by management.
- Monitoring by reviewers of changes in eligibility determinations to ensure that overrides in determination process are appropriate.
- Periodic audits of detailed transactions.

APPENDIX 4.2D5

EQUIPMENT AND REAL PROPERTY MANAGEMENT

Description of Compliance Requirement

Equipment Management - Title to equipment acquired by a non-Federal entity with Federal awards vests with the non-Federal entity. Equipment means tangible nonexpendable property, including exempt property, charged directly to the award having a useful life of more than one year and an acquisition cost of $5000 or more per unit. However, consistent with a non-Federal entity's policy, lower limits may be established.

Real Property Management - Title to real property acquired by non-Federal entities with Federal awards vests with the non-Federal entity. Real property shall be used for the originally authorized purpose as long as needed for that purpose. For non-Federal entities covered by OMB Circular A-110 and with written approval from the Federal awarding agency, the real property may be used in other federally sponsored projects or programs that have purposes consistent with those authorized for support by the Federal awarding agency. The non-Federal entity may not dispose of or encumber the title to real property without the prior consent of the awarding agency.

Equipment and Real Property Management requirements applies to Federal programs which purchase equipment or real property.

Control Objectives

To provide reasonable assurance that proper records are maintained for equipment acquired with Federal awards, equipment is adequately safeguarded and maintained, disposition or encumbrance of any equipment or real property is in accordance with Federal requirements, and the Federal awarding agency is appropriately compensated for its share of any property sold or converted to non-Federal use.

Controls:

- Accurate records maintained on all acquisitions and dispositions of property acquired with Federal awards.
- Property tags are placed on equipment.
- A physical inventory of equipment is periodically taken and compared to property records which includes a description with a serial number or other identification number, source, who holds title, acquisition date and cost, percentage of Federal participation in the cost, location, condition, and disposition data.
- Procedures established to ensure that the Federal awarding agency is appropriately reimbursed for dispositions of property acquired with Federal awards.
- Policies and procedures in place for responsibilities of recordkeeping and authorities for disposition.
- Accounting system provides for separate identification of property acquired wholly or partly with Federal funds and with non-Federal funds.
- Program managers are provided with applicable requirements and guidelines.
- Management reviews the results of periodic inventories and follows up on inventory discrepancies.
- Management reviews dispositions of property to ensure appropriate valuation and reimbursement to Federal awarding agencies.

APPENDIX 4.2D6

MATCHING, LEVEL OF EFFORT, EARMARKING

Description of Compliance Requirement

The specific requirements for matching, level of effort, and earmarking are unique to each Federal program and are found in the laws, regulations, and the provisions of contract or grant agreements pertaining to the program.

Matching or cost sharing includes requirements to provide contributions (usually non-Federal) of a specified amount or percentage to match Federal awards. Matching may be in the form of allowable costs incurred or in-kind contributions (including third-party in-kind contributions).

Level of effort includes requirements for (a) a specified level of service to be provided from period to period, (b) a specified level of expenditures from non-Federal or Federal sources for specified activities to be maintained from period to period, and (c) Federal funds to supplement and not supplant non-Federal funding of services.

Earmarking includes requirements that specify the minimum and/or maximum amount or percentage of the program's funding that must/may be used for specified activities, including funds provided to subrecipients. Earmarking may also be specified in relation to the types of participants covered.

Control Objectives

To provide reasonable assurance that matching, level of effort, or earmarking requirements are met using only allowable funds or costs which are properly calculated and valued.

Controls:

- Official written policy exists outlining:
  - Responsibilities for determining required amounts or limits for matching, level of effort, or earmarking.
  - Methods of valuing matching requirements, e.g., "in-kind" contributions of property and services, calculations of levels of effort.
  - Allowable costs that may be claimed for matching, level of effort, or earmarking.
  - Methods of accounting for and documenting amounts used to calculate amounts claimed for matching, level of effort, or earmarking.
- Evidence obtained such as a certification from the donor, or other procedures performed to identify whether matching contributions:
  - Are from non-Federal sources.
  - Involve Federal funding, directly or indirectly.
  - Were used for another federally-assisted program.

  Note: Generally, matching contributions must be from a non-Federal source and may not involve Federal funding or be used for another federally assisted program.

- Adequate review of monthly cost reports and adjusting entries.
- Accounting system capable of:
  - Separately accounting for data used to support matching, level of effort, or earmarking amounts or limits or calculations.
  - Ensuring that expenditures or expenses, refunds, and cash receipts or revenues are properly classified and recorded only once as to their effect on matching, level of effort, or earmarking.
  - Documenting the value of "in-kind" contributions of property or services, including:
    Basis for local labor market rates for valuing volunteer services.
    Payroll records or confirmation from other organizations for services provided by their employees.
    Quotes, published prices, or independent appraisals used as the basis for donated equipment, supplies, land, buildings, or use of space.
- Supervisory review of matching, level of effort, or earmarking activities performed to assess the accuracy and allowability of transactions and determinations, e.g., at the time reports on Federal awards are prepared.

APPENDIX 4.2D7

PERIOD OF AVAILABILITY OF FEDERAL FUNDS

Description of Compliance Requirement

Federal awards may specify a time period during which the non-Federal entity may use the Federal funds. Where a funding period is specified, a non-Federal entity may charge to the award only costs resulting from obligations incurred during the funding period and any pre-award costs authorized by the Federal awarding agency. Also, if authorized by the Federal program, unobligated balances may be carried over and charged for obligations of a subsequent funding period. Obligations means the amounts of orders placed, contracts and subgrants awarded, goods and services received, and similar transactions during a given period that will require payment by the non-Federal entity during the same or a future period.

Non-Federal entities shall liquidate all obligations incurred under the award not later than 90 days after the end of the funding period (or as specified in a program regulation). The Federal agency may extend this deadline upon request.

Control Objectives

To provide reasonable assurance that Federal funds are used only during the authorized period of availability.

Controls:

- The budgetary process considers period of availability of Federal funds as to both obligation and disbursement.
- Accounting system prevents obligation or expenditure of Federal funds outside of the period of availability.
- Review of disbursements by person knowledgeable of period of availability of funds.
- End of grant period cut-offs are met by such mechanisms as advising program managers of impending cut-off dates and review of expenditures just before and after cut-off date.
- Cancellation of unliquidated commitments at the end of the period of availability.
- Timely communication of period of availability requirements and expenditure deadlines to individuals responsible for program expenditure, including automated notifications of pending deadlines.
- Periodic reporting of unliquidated balances to appropriate levels of management and follow up.
- Periodic review of expenditures before and after cut-off date to ensure compliance with period of availability requirements.
- Review by management of reports showing budget and actual for period.

PROCUREMENT AND SUSPENSION AND DEBARMENT

Description of Compliance Requirement

Procurement - States, and governmental subrecipients of States, shall use the same State policies and procedures used for procurements from non-Federal funds. They also shall ensure that every purchase order or other contract includes any clauses required by Federal statutes and executive orders and their implementing regulations.

Institutions of higher education, hospitals, and other non-profit organizations shall use procurement procedures that conform to applicable Federal law and regulations and standards identified in OMB Circular A-110. All non-Federal entities shall follow Federal laws and implementing regulations applicable to procurements, as noted in Federal
agency implementation of the A-102 Common Rule and OMB Circular A-110.

In addition to those statutes listed in the A-102 Common Rule and OMB Circular A-110, Section 1605 of ARRA prohibits the use of ARRA funds for a project for the construction, alteration, maintenance, or repair of a public building or work unless all of the iron, steel, and manufactured goods used in the project are produced in the United States. ARRA provides for waiver of these requirements under specified circumstances. An award term is required in all ARRA-funded awards for construction, alteration, maintenance, or repair of a public building or public work.
Suspension and Debarment - Non-Federal entities are prohibited from contracting with or making subawards under covered transactions to parties that are suspended or debarred or whose principals are suspended or debarred. Covered transactions include those procurement contracts for goods and services awarded under a nonprocurement transaction (e.g., grant or cooperative agreement) that are expected to equal or exceed $25,000 or meet certain other specified criteria.

All nonprocurement transactions (i.e., subawards to subrecipients), irrespective
of award amount, are considered covered transactions.

Control Objectives

To provide reasonable assurance that procurement of goods and services are made in compliance with the provisions of the A-102 Common Rule or OMB Circular A-110, as applicable, and that covered transactions (as defined in the suspension and debarment common rule) are not made with a debarred or suspended party.

Controls:

- Board or governing body oversight required for high dollar, lengthy, or other sensitive procurement contracts.
- Procurement manual that incorporated Federal requirements.
- Clear assignment of authority for issuing purchasing orders and contracting for goods and
- Conflict-of-interest statements are maintained for individuals with responsibility for procurement of goods or services.
- Contractor's performance with the terms, conditions, and specifications of the contract is monitored and documented.

- Establish segregation of duties between employees responsible for contracting and accounts payable and cash disbursing.
- Procurement actions appropriately documented in the procurement files.
- Supervisors review procurement and contracting decisions for compliance with Federal procurement policies.

- Procedures established to verify that vendors providing goods and services under the award have not been suspended or debarred by the Federal Government.
- Official written policy for procurement and contracts establishing:
  - Contract files that document significant procurement history.
  - Methods of procurement, authorized including selection of contract type, contractor selection or rejection, and the basis of contract price.
  - Verification that procurements provide full and open competition.
  - Requirements for cost or price analysis, including for contract modifications.
  - Obtaining and reacting to suspension and debarment certifications.
  - Other applicable requirements for procurements under Federal awards are followed.
- Official written policy for suspension and debarment that:
  - Contains or references the Federal requirements;
  - Prohibits the award of a subaward, covered contract, or any other covered agreement for program administration, goods, services, or any other program purpose with any suspended or debarred party; and
  - Requires staff to determine that entities receiving subawards of any value and procurement contracts equal to or exceeding $25,000 and their principals are not suspended or debarred, and specifies the means that will be used to make that determination, i.e., checking the *Excluded Parties Listing System* (EPLS), which is maintained by the General Services Administration; obtaining a certification; or inserting a clause in the agreement.
- A system in place to assure that procurement documentation is retained for the time period required by the A-102 Common Rule, OMB Circular A-110 (2 CFR part 215), award agreements, contracts, and program regulations. Documentation includes:
  - The basis for contractor selection;
  - Justification for lack of competition when competitive bids or offers are not obtained; and
  - The basis for award cost or price.
- Procurement staff is provided a current hard-copy *EPLS* or have on-line access.
- Management periodically conducts independent reviews of procurements and contracting activities to determine whether policies and procedures are being followed as intended.

APPENDIX 4.2D9

PROGRAM INCOME

Description of Compliance Requirement

Program income is gross income received that is directly generated by the federally funded project during the grant period. If authorized by Federal regulations or the grant agreement, costs incident to the generation of program income may be deducted from gross income to determine program income. Program income includes, but is not limited to, income from fees for services performed, the use or rental of real or personal property acquired with grant funds, the sale of commodities or items fabricated under a grant agreement, and payments of principal and interest on loans made with grant funds.

Control Objectives

To provide reasonable assurance that program income is correctly earned, recorded, and used in accordance with the program requirements.

Controls:

- Pricing and collection policies procedures clearly communicated to personnel responsible for program income.
- Mechanism in place to ensure that program income is properly recorded as earned and deposited in the bank as collected.
- Policies and procedures provide for correct use of program income in accordance with Federal program requirements.
- Internal audit of program income.
- Management compares program income to budget and investigates significant differences.

APPENDIX 4.2D10

REAL PROPERTY ACQUISITION AND RELOCATION ASSISTANCE

Description of Compliance Requirement

The Uniform Relocation Assistance and Real Property Acquisition Policies Act of 1970, as amended, (URA) provides for uniform and equitable treatment of persons displaced by Federally-assisted programs from their homes, businesses, or farms. Federal requirements govern the determination of payments for replacement housing assistance, rental assistance and down payment assistance for individuals displaced by federally funded projects. The regulations also cover the payment of moving-related expenses and reestablishment expenses incurred by displaced businesses and farm operations.

Control Objectives

To provide reasonable assurance of compliance with the real property acquisition, appraisal, negotiation, and relocation requirements.

Controls:

- Employees handling relocation assistance and real property acquisition have been trained in the requirements of the URA.
- Review of expenditures pertaining to real property acquisition and relocation assistance by employees knowledgeable in the URA.
- A system is in place to adequately document relocation assistance and real property acquisition.
- Management monitors relocation assistance and real property acquisition for compliance with the URA.

APPENDIX 4.2D11

REPORTING

Description of Compliance Requirement

Financial Reporting - When applicable, recipients should use the standard financial reporting forms or such other forms as may be authorized by OMB (approval is indicated by an OMB paperwork control number on the form). Each recipient must report program outlays and program income on a cash or accrual basis, as prescribed by the Federal awarding agency.

Performance Reporting - When applicable, Recipients shall submit performance reports at least annually but not more frequently than quarterly. Performance reports generally contain, for each award, brief information of the following types:

1. A comparison of actual accomplishments with the goals and objectives established for the period.
2. Reasons why established goals were not met, if appropriate.
3. Other pertinent information including, when appropriate, analysis and explanation of cost overruns or high unit costs.

Special Reporting - Non-Federal entities may be required to submit other reporting which may be used by the Federal agency for such purposes as allocating program funding.

Control Objectives

To provide reasonable assurance that reports of Federal awards submitted to the Federal awarding agency or pass-through entity include all activity of the reporting period, are supported by underlying accounting or performance records, and are fairly presented in accordance with program requirements.

Controls:

- Written policy exists that establishes responsibility and provides the procedures for periodic monitoring, verification, and reporting of program progress and accomplishments.
- Tracking system which reminds staff when reports are due.
- The general ledger or other reliable records are the basis for the reports.
- Supervisory review of reports performed to assure accuracy and completeness of data and information included in the reports.
- The required accounting method is used (e.g., cash or accrual).
- Communications from external parties corroborate information included in the reports for Federal awards.
- Periodic comparison of reports to supporting records.

APPENDIX 4.2D12

SUBRECIPIENT MONITORING

Description of Compliance Requirement

A pass-through entity is responsible for:

- Award Identification – At the time of the award, identifying to the subrecipient the Federal award information (i.e., CFDA title and number; award name and number; if the award is research and development; and name of Federal awarding agency) and applicable compliance requirements.

- During-the-Award Monitoring – Monitoring the subrecipient's use of Federal awards through reporting, site visits, regular contact, or other means to provide reasonable assurance that the subrecipient administers Federal awards in compliance with laws, regulations, and the provisions of contracts or grant agreements and that performance goals are achieved.

- Subrecipient Audits – (1) Ensuring that subrecipients expending $500,000 or more in Federal awards during the subrecipient's fiscal year for fiscal years ending after December 31, 2003 as provided in OMB Circular A-133 have met the audit requirements of OMB Circular A-133 (the circular is available on the Internet at http://www.whitehouse.gov/omb/circulars/a133/a133.html) and that the required audits are completed within 9 months of the end of the subrecipient's audit period; (2) issuing a management decision on audit findings within 6 months after receipt of the subrecipient's audit report; and (3) ensuring that the subrecipient takes timely and appropriate corrective action on all audit findings. In cases of continued inability or unwillingness of a subrecipient to have the required audits, the pass-through entity shall take appropriate action using sanctions.

- Pass-Through Entity Impact – Evaluating the impact of subrecipient activities on the pass-through entity's ability to comply with applicable Federal regulations.

- Central Contractor Registration – Identifying to first-tier subrecipients the requirement to register in the Central Contractor Registration, including obtaining a Dun and Bradstreet Data Universal Numbering System (DUNS) number, and maintain the currency of that information.

Control Objectives

To provide reasonable assurance that Federal award information and compliance requirements are identified to subrecipients, subrecipient activities are monitored, subrecipient audit findings are resolved, and the impact of any subrecipient noncompliance on the pass-through entity is evaluated. Also, the pass-through entity should perform procedures to provide reasonable assurance that the subrecipient obtained required audits and takes appropriate corrective action on audit findings.

Controls:

- Subrecipients:
  - Are willing and able to comply with the requirements of the award, and
  - Have accounting systems, including the use of applicable cost principles, and internal control systems adequate to administer the award.

- Identify to subrecipients the Federal award information (e.g., CFDA title and number, award name, name of Federal agency, amount of award) and applicable compliance requirements.
- Include in agreements with subrecipients the requirement to comply with the compliance requirements applicable to the Federal program, including the audit requirements of OMB Circular A-133.
- Subrecipients' compliance with audit requirements monitored using techniques such as the following:
  - Determining by inquiry and discussions whether subrecipient met thresholds requiring an audit under OMB Circular A-133.
  - If an audit is required, assuring that the subrecipient submits the report, report package or the documents required by OMB circulars and/or recipient's requirements.
  - If a subrecipient was required to obtain an audit in accordance with OMB Circular A-133 but did not do so, following up with the subrecipient until the audit is completed. Taking appropriate actions such as withholding further funding until the subrecipient meets the audit requirements.
- Subrecipient's compliance with Federal program requirements monitored using such techniques as the following:
  - Issuing timely management decisions for audit and monitoring findings to inform the subrecipient whether the corrective action planned is acceptable.
  - Maintain a system to track and following-up on reported deficiencies related to programs funded by the recipient and ensure that timely corrective action is taken.
  - Regular contacts with subrecipients and appropriate inquiries concerning the Federal program.
  - Reviewing subrecipient reports and following-up on areas of concern.
  - Monitoring subrecipient budgets.
  - Performing site visits to subrecipient to review financial and programmatic records and observe operations.
  - Offering subrecipients technical assistance where needed.
- Standard award documents used by the non-Federal entity contain:
  - Specifically listed in the award document, attached as an exhibit to the document, or incorporated by reference to specific criteria.
  - The description and program number for each program as stated in the CFDA. If the program funds include pass-through funds from another recipient, the pass-through program information should also be identified.
  - A statement signed by an official of the subrecipient, stating that the subrecipient was informed of, understands, and agrees to comply with the applicable compliance requirements.
- Establish a tracking system to assure timely submission of required reporting, such as: financial reports, performance reports, audit reports, onsite monitoring reviews of subrecipients, and timely resolution of audit findings.
- Supervisory reviews performed to determine the adequacy of subrecipient monitoring.

APPENDIX 5.1
IT GENERAL CONTROLS

Providing information to enable management's reporting to key stakeholders is a life cycle of collecting complete and accurate information and reporting it on a timely basis. As one might expect, this life cycle is highly dependent on information systems, such as applications, databases and other tools used to enhance the efficiency and effectiveness of data processing. The balance of this appendix is dedicated to providing guidance on IT controls that are specifically designed to support financial reporting objectives. These controls are not intended to be an exhaustive list. However, they do provide a starting point as agencies determine which IT controls are necessary for their environment. Consideration should also be given to IT controls that may not be included below, but which an agency considers relevant nonetheless. The most relevant internal controls applicable to financial statement assertions can be defined to include activities that prevent or detect and correct a significant misstatement in the financial reporting or other required disclosures, including those over recording amounts into the general ledger and recording journal entries (standard, nonstandard and consolidation). The most relevant controls may be manual or automated, and preventive or detective in nature.

As noted previously, this guidance is not intended to be authoritative. Professional judgment needs to be applied when determining the necessary controls that should be included in the compliance program, including some which may not be highlighted as most relevant controls in this document.

Note: The documentation noted below is from the IT Governance Institute (ITGI), IT Control Objectives For Sarbanes Oxley – "THE ROLE OF IT IN THE DESIGN AND IMPLEMENTATION OF INTERNAL CONTROL OVER FINANCIAL REPORTING (2ND EDITION)".

APPENDIX 5.1A – OPTION 1

IT General Controls
Fiscal Year End June 30, 20XX

Note: The scope of this review is limited to only those applications and systems used in the business processes that were determined to be High or Moderate. Thus, if it is determined that no automated or IT-dependent manual controls are in scope for a given account or process, management need not test the related ITGCs.

Acquire and Maintain Application Software (AI2)

Control Objective: Controls provide reasonable assurance that application and system software is acquired or developed that effectively supports financial reporting requirements.

Rationale: The process of acquiring and maintaining software includes the design, acquisition/building and deployment of systems that support the achievement of business objectives. This process includes major changes to existing systems. This is where controls are designed and implemented to support initiating, recording, processing and reporting financial information and disclosure. Deficiencies in this area may have a significant impact on financial reporting and disclosure. For instance, without sufficient controls over application interfaces, financial information may not be complete or accurate.

IT General Controls supporting control objective:

IT General Control	Tests of Controls	COBIT References (4.1)	Test Results/Comments	W/P References
1. The organization has a system development life cycle (SDLC) methodology, which includes security and processing integrity requirements of the organization.	Obtain a copy of the organization's SDLC methodology to determine that it addresses security and processing integrity requirements. Consider whether there are appropriate steps to determine if these requirements are considered throughout the development or acquisition life cycle, e.g., security and processing integrity are considered during the requirements phase.	PO8.3 AI2.3 AI2.4		

2. The SDLC methodology includes requirements that information systems be designed to include application controls that support complete, accurate, authorized and valid transaction processing.	Review the SDLC methodology to determine if it addresses application controls. Consider whether there are appropriate steps so that application controls are considered throughout the development or acquisition life cycle, e.g., application controls should be included in the conceptual design and detail design phases.	AI1 AI2.3 AC		
3. To maintain a reliable environment, IT management involves users in the design of applications, selection of packaged software and testing thereof.	Review the SDLC methodology to determine if users are appropriately involved in the design of applications, selection of packaged software and testing.	AI1 AI2.1 AI2.2 AI7.2		
4. The organization acquires/develops application systems software in accordance with its acquisition, development and planning process.	Select a sample of projects that resulted in new financial systems being implemented. Review the documentation and deliverables from these projects to determine if they have been completed in accordance with the acquisition, development and planning processes.	AI2		

Enable Operations (PO6, PO8, AI6, DS13)

Control Objective: Controls provide reasonable assurance that policies and procedures that define required acquisition and maintenance processes have been developed and are maintained, and that they define the documentation needed to support the proper use of the applications and the technological solutions put in place.

Rationale: Policies and procedures include the SDLC methodology and the process for acquiring, developing and maintaining applications as well as required documentation. For some organizations, the policies and procedures

include service level agreements, operational practices and training materials. Policies and procedures support an organization's commitment to perform business process activities in a consistent and objective manner.

IT General Control	Tests of Controls	COBIT References (4.1)	Test Results/Comments	W/P References
5. The organization has policies and procedures regarding program development, program change, access to programs and data, and computer operations, which are periodically reviewed, updated and approved by management.	Confirm that the organization has policies and procedures that are reviewed and updated regularly for changes in the business. When policies and procedures are changed, determine if management approves such changes. Select a sample of projects and determine that user reference and support manuals, systems documentation and operations documentation were prepared. Consider whether drafts of these manuals were incorporated in user acceptance testing. Determine whether any changes to proposed controls resulted in documentation updates.	PO6.1 PO6.3 PO8.1 PO8.2 PO8.3 AI6.1 D13.1		
6. The organization develops maintains and operates its systems and applications in accordance with its supported, documented policies and procedures.	Obtain the policies and procedures and determine if the organization manages its IT environment in accordance with them.	PO6.1 PO6.3 PO8.1 PO8.2 AI6.1 DS13.1		

Install and Accredit Solutions and Changes (AI7)

Control Objective: Controls provide reasonable assurance that the systems are appropriately tested and validated prior to being placed into production processes and that associated controls operate as intended and support financial reporting requirements.

Rationale: Installation testing and validating relate to the migration of new systems into production. Before such systems are installed, appropriate testing and validation should be performed to determine if the systems are

operating as designed. Without adequate testing, systems may not function as intended and may provide invalid information, which could result in unreliable financial information and reports.

IT General Control	Tests of Controls	COBIT References (4.1)	Test Results/Comments	W/P References
7. A testing strategy is developed and followed for all significant changes in applications and infrastructure technology, which addresses unit, system, integration and user acceptance-level testing so that deployed systems operate as intended.	Select a sample of systems development projects and significant system upgrades (including technology upgrades). Determine if a formal testing strategy was prepared and followed. Consider whether this strategy considered potential development and implementation risks and addressed all the necessary components to address these risks, e.g., if the completeness and accuracy of system interfaces are essential to the production of complete and accurate reporting, these interfaces were included in the testing strategy. (Note: Controls over the final move to production are addressed in *Manage Changes*)	AI7.2 AI7.4 AI7.6 AI7.7		
8. Interfaces with other systems are tested to confirm that data transmissions are complete, accurate and valid.	Select a sample of system development projects and system upgrades that are significant for financial reporting. Determine if interfaces with other systems were tested to confirm that data transmissions are complete, e.g., record totals are accurate and valid. Consider whether the extent of testing was sufficient and included recovery in the event of incomplete data transmissions.	AI7.5		

Manage Changes (AI6, AI7)

Control Objective: Controls provide reasonable assurance that system changes of financial reporting significance are authorized and appropriately tested before being moved to production.

Rationale: Managing changes addresses how an organization modifies system functionality to help the business meet its financial reporting objectives. Deficiencies in this area could significantly impact financial reporting. For instance, changes to the programs that allocate financial data to accounts require appropriate approvals and testing prior to the change so that proper classification and reporting integrity is maintained.

IT General Control	Tests of Controls	COBIT References (4.1)	Test Results/Comments	W/P References
9. Requests for program changes, system changes and maintenance (including changes to system software) are standardized, logged, approved, documented, and subject to formal change management procedures.	Determine that a documented change management process exists and is maintained to reflect the current process. Consider if change management procedures exist for all changes to the production environment, including program changes, system maintenance and infrastructure changes. Evaluate the process used to control and monitor change requests. Consider whether change requests are properly initiated, approved and tracked. Determine whether program change is performed in a segregated, controlled environment. Select a sample of changes made to applications/systems to determine whether they were adequately tested and approved before being placed into a production environment. Establish if the following are included in the approval process: operations, security, IT infrastructure	AI6.1 AI6.2 AI6.4 AI6.5 AI7.3 AI7.8 AI7.9 AI7.10 AI7.11		

	management and IT management. Evaluate procedures designed to determine that only authorized/approved changes are moved into production. Trace the sample of changes back to the change request log and supporting documentation. Confirm that these procedures address the timely implementation of patches to system software. Select a sample to determine compliance with the documented procedures.			
10. Emergency change requests are documented and subject to formal change management procedures.	Determine if a process exists to control and supervise emergency changes. Determine if an audit trail exists of all emergency activity and verify that it is independently reviewed. Determine that procedures require emergency changes to be supported by appropriate documentation. Establish that backout procedures developed for emergency changes. Evaluate procedures ensuring that all emergency changes are tested and subject to standard approval procedures after they have been made. Review a sample of changes that are recorded as "emergency" changes, and determine if they contain the needed approval and the needed	AI6.3 AI7.10		

	access was terminated after a set period of time. Establish that the sample of changes was well documented.			
11. Controls are in place to restrict migration of programs to production by authorized individuals only.	Evaluate the approvals required before a program is moved to production. Consider approvals from system owners, development staff and computer operations. Confirm that there is appropriate segregation of duties between the staff responsible for moving a program into production and development staff. Obtain and test evidence to support this assertion.	AI7.8		

Ensure System Security (DS5)

Control Objective: Controls provide reasonable assurance that financial reporting systems and subsystems are appropriately secured to prevent unauthorized use, disclosure, modification, damage or loss of data.

Rationale: Managing systems security includes both physical and logical controls that prevent unauthorized access. These controls typically support authorization, authentication, nonrepudiation, data classification and security monitoring. Deficiencies in this area could significantly impact financial reporting. For instance, insufficient controls over transaction authorization may result in inaccurate financial reporting.

IT General Control	Tests of Controls	COBIT References (4.1)	Test Results/Comments	W/P References
12. An information security policy exists and has been approved by an appropriate level of executive management.	Obtain a copy of the organization's security policy and evaluate the effectiveness. Points to be taken into consideration include: • Is there an overall statement of the importance of security to the organization? • Have specific policy objectives been defined? • Have employee and contractor security responsibilities been addressed? • Has the policy been approved by	PO6.3 PO6.5 PO5.2	.	

	an appropriate level of senior management to demonstrate management's commitment to security? • Is there a process to communicate the policy to all levels of management and employees?			
13. Procedures exist and are followed to authenticate all users of the system (both internal and external) to support the existence of transactions.	Assess the authentication mechanisms used to validate user credentials for financial reporting systems and subsystems and validate that user sessions time-out after the predetermined period of time. Validate that no shared user profiles (including administrative profiles) are used.	DS5.3 AC		
14. Procedures exist and are followed to maintain the effectiveness of authentication and access mechanisms (e.g., regular password changes)	Review the security practices to confirm that authentication controls (passwords, IDs, two-factor, etc.) are used appropriately and are subject to common confidentiality requirements (IDs and passwords not shared, alphanumeric passwords used, etc.).	DS5.3 DS5.4		

15. Procedures exist and are followed relating to timely action for requesting, establishing, issuing, suspending and closing user account. (Include procedures for authenticating transactions originating outside the organization.)	Confirm that procedures for the registration, change and deletion of users from financial reporting systems and subsystems on a timely basis exist and are followed. Select a sample of new users and determine if management approved their access and the access granted agrees with the access privileges that were approved. Select a sample of terminated employees and determine if their access has been removed, and the removal was done in a timely manner. Select a sample of privileged and current users and review their access for appropriateness based upon their job functions.	DS5.4		
16. A control process exists and is followed to periodically review and confirm access rights.	Inquire whether access controls for financial reporting systems and subsystems are reviewed by management on a periodic basis. Assess the adequacy of how exceptions are reexamined, and if the follow-up occurs in a timely manner.	DS5.4		

17. IT security administration monitors and logs security activity at the operating systems, application and datable levels and identified security violations are reported to senior management.	Inquire whether a security office exists to monitor for security vulnerabilities at the application and database levels and related threat events. Asses the nature and extent of such events over the past year and discuss with management how they have responded with controls to prevent unauthorized access or manipulation of financial systems and subsystems. Validate that attempts to gain unauthorized access to financial reporting systems and subsystems are logged and follow up on a timely basis.	DS5.5		
18. Controls relating to appropriate segregation of duties over requesting and granting access to systems and data exist and are followed.	Review the process to request and grant access to systems and data and confirm that the same person does not perform these functions.	DS5.3 DS5.4		

Manage the Configuration (DS9)

Control Objective: Controls provide reasonable assurance that IT components, as they relate to security and processing, are well protected, would prevent any unauthorized changes, and assist in the verification and recording of the current configuration.

Rationale: Configuration management includes procedures such that security and processing integrity controls are set up in the system and maintained through its life cycle. Insufficient configuration controls can lead to security exposures that may permit unauthorized access to systems and data and impact financial reporting. An additional potential risk is corruption to data integrity caused by poor control of the configuration when making system changes or by the introduction of unauthorized system components.

IT General Control	Tests of Controls	COBIT References (4.1)	Test Results/Comments	W/P References
19. Application software and data storage systems are properly configured to provision access based on the individual's demonstrated need to view, add, change or delete data.	Conduct an evaluation of the frequency and timeliness of management's review of configuration records. Assess whether management has documented the configuration management procedures. Review a sample of configuration changes, additions or deletions, to consider if they have been properly approved based on a demonstrated need.	DS5.4		

Manage Problems and Incidents (DS8, DS10)

Control Objective: Controls provide reasonable assurance that any problems and/or incidents are properly responded to, recorded, resolved or investigated for proper resolution.

Rationale: The process of managing problems and incidents addresses how an organization identifies documents and responds to events that fall outside of normal operations. Deficiencies in this area could significantly impact financial reporting.

IT General Control	Tests of Controls	COBIT References (4.1)	Test Results/Comments	W/P References
20. IT management has defined and implemented an incident and problem management system such that data integrity and access control incidents are recoded, analyzed, resolved in a timely manner and reported to management.	Determine if an incident management system exists and how it is being used. Review how management has documented how the system is to be used. Review a sample of incident reports, to consider if the issues were addressed (recorded, analyzed and resolved) in a timely manner.	DS8		

Manage Data (DS11)

Control Objective: Controls provide reasonable assurance that data recorded, processed and reported remain complete, accurate and valid throughout the update and storage process.

Rationale: Managing data includes the controls and procedures used to support information integrity, including its completeness, accuracy, authorization and existence. Controls are designed to support initiating, recording, processing and reporting financial information. Deficiencies in this area could significantly impact financial reporting. For instance, without appropriate authorization controls over the initiation of transactions, resulting financial information may not be reliable.

IT General Control	Tests of Controls	COBIT References (4.1)	Test Results/Comments	W/P References
21. Management has implemented a strategy for cyclical backup of data and programs.	Determine if the organization has procedures in place to back up data and programs based on IT and user requirements. Select a sample of data files and programs and determine if they are being backed up as required.	DS11.5		
22. The restoration of information is periodically tested.	Inquire whether the retention and storage of messages, documents, programs, etc., have been tested during the past year. Obtain and review the results of testing activities. Establish whether any deficiencies were noted and whether they have been reexamined. Obtain the organization's access security policy and discuss with those responsible whether they follow such standards and guidelines dealing with sensitive backup data.	DS11.5		

Manage Operations (DS13)

Control Objective: Controls provide reasonable assurance that authorized programs are executed as planned and deviations from scheduled processing are identified and investigated, including controls over job scheduling, processing and error monitoring.

Rationale: Managing operations addresses how an organization maintains reliable application systems in support of the business to initiate record, process and report financial information. Deficiencies in this area could significantly impact an entity's financial reporting. For instance, lapses in the continuity of application systems may prevent an organization from recording financial transactions and thereby undermine its integrity.

IT General Control	Tests of Controls	COBIT References (4.1)	Test Results/Comments	W/P References
23. Management has established, documented and follows standard procedures for IT operations, including job scheduling and monitoring and responding to security and processing integrity events.	Determine if management has documented its procedures for IT operations, and operations are reviewed periodically for compliance. Review a sample of events to confirm that response procedures are operating effectively. When used, review the job scheduling process and the procedures in place to monitor job completeness.	DS13.1 DS13.2		

END-USER COMPUTING CONTROLS

The following illustrative controls for End-User Computing are presented to address the characteristics of a typical End-User Computing environment. Appropriate COBIT processes apply to this environment.

End-User Computing Control	Test of Controls	Test Results/Comments	W/P References
End-User Computing policies and procedures concerning security and processing integrity exist and are followed.	Obtain a copy of the End-User Computing policies and procedures and confirm that they address security and processing integrity controls.		

End-User Computing, including spreadsheets and other user-developed programs, are documented and regularly reviewed for processing integrity, including their ability to sort, summarize and report accurately.	Inquire as to management's knowledge of End-User programs in use across the agency. Inquire as to the frequency and approaches followed to review End-User programs for processing integrity, and review a sample of these to confirm effectiveness. Review user-developed systems and test their ability to sort, summarize and report in accordance with management intentions.		
User-developed systems and data are regularly backed up and stored in a secure area.	Inquire how End-User systems are backed up and where they are stored.		
User-developed systems, such as spreadsheets and other end-user programs, are secured from unauthorized use.	Review the security used to protect unauthorized access to use-developed systems. Consider observing a user attempting to gain unauthorized access to user-developed systems. Inquire how management is able to detect unauthorized access and what follow-up procedures are performed to assess the impact of such access. Select a sample of user-developed systems and determine who has access and if the access is appropriate.		
Inputs, processing and outputs from user-developed systems are independently verified for completeness and accuracy.	Inquire how management verifies the accuracy and completeness of information processed and reported from user-developed systems. Inquire as to who review and approves outputs from user-developed systems prior to their submission for further processing or final reporting. Consider reperforming or reviewing the logic used in user-developed systems and conclude on their ability to process completely and accurately.		

APPENDIX 5.1B OPTION 2

IT General Controls
Fiscal Year End June 30, 20XX

Note: The scope of this review is limited to only those applications and systems used in the business processes that were determined to be High or Moderate Risk. Thus, if it is determined that no automated or IT-dependent manual controls are in scope for a given account or process, management need not test the related ITGCs.

Management's assessment should also include IT General Controls (ITGCs). ITGCs relative to the Manage Change, Logical Access and Other ITGCs have pervasive effect on preventing or detecting and correcting material misstatements in the financial statements, and are controls which the operating effectiveness of other controls depend. Agency will need to identify and understand ITGCs related to the Manage Change, Logical Access and Other ITGC, where applicable, for purposes of the self-assessment review of internal control over financial reporting.

ITGCs consist of three categories:

- Manage Change
- Logical Access
- Other ITGCs

Overall Objective of Manage Change
Only appropriately authorized, tested and approved changes are made to applications, interfaces, databases, and operating systems.

Authorizing, Testing, and Approving Changes
For purposes of testing for the manage change ITGCs, the following definitions are used:

- Authorized – Determine that the change requested has been appropriately authorized. Depending on the agency's policy and in some situations, such as minor changes, perhaps defined as those requiring less than a certain number of hours of programmer time, changes may not require specific authorizations.
- Tested – Determine whether users performed testing to confirm the change functions as intended. Otherwise confirm that other appropriate testing did occur. In some situations, such as infrastructure changes, IT only testing may be acceptable depending on the agency's policy.
- Approved – Determine if application owners and IT personnel approved, changes prior to being moved into production. In some situations, such as infrastructure changes.

Types of Manage Changes
In order to determine the most appropriate testing approach, the agency needs to understand and document the different processes used for managing changes. Documentation (including walkthroughs) may include the different processes for the following types of changes:

- Program Development/Acquisition – Development and implementation of new applications or interfaces.
- Program Change – Changes being made to existing applications and interfaces.
- Maintenance to System Software – Technical changes made to the Database Management System, operating systems, and other system software (e.g. patches and upgrades).
- Emergency Changes – Changes made in an emergency situation.
- Configuration/Parameter Changes – Relates to changes being made to the overall configuration and parameter settings to the various technical components of the IT environment. This includes the initial setup of the configuration settings for new applications.

Technical Components of the IT Environment

During the risk assessment process, agency determined which of the following technical components of the IT environment affect the Manage Change Category and are in scope for testing:

- Applications
- Interfaces (IT controlled)
- Database Management System
- Operating Systems/Networks

Identifying Changes to IT Environment (Testing Population)

Based on the test approach defined, obtain a complete list of the changes to the IT environment for any high or moderate processes from July 1st through the date of the test (change management test).

- The preferred method of selecting a change management sample is to obtain a list directly from a change management system that indicates all changes actually made from July 1st through the date of the test. Determine that the list of changes is complete.
- In the event a system generated list is not available, then a combination of the following may be considered:
    - Obtain a list of changes made (either a manually maintained list or from an automated tracking system).
    - Determine that the list of programs changes is complete. Obtain a list of actual changes by looking for executable modules with a compile date within the period (in many cases this may only be the last change to the module; however, for purposes of the completeness test, this is adequate). Select a sample of changes during the period from this list and verify that the change is on the list of changes obtained.
- If there are no changes, determine that changes have not occurred by checking that the last compile date for the in scope technical components were not during July 1st through the date of the test.

Compensating Control for Manage Change Segregation of Duties

In cases where manage change segregation of incompatible duties cannot be attained due to organizational structures or other reasons, a compensating control can be used to provide

assurance that no unauthorized program or data changes are occurring. The compensating control should be designed to detect when the other manage change ITGC controls in place have been circumvented because of the segregation of incompatible duties issues. Examples of compensating ITGCs are:

- Change log review to determine that only approved changes were moved into production, while confirming the change log is complete.
- Change control meetings that discuss and follow-up on recent changes that have been moved into production.

Certain change types may not lend themselves to segregation of incompatible duties (e.g., minor patches to operating system).

Complete the Manage Change Testing Table.

Manage Change	Tests of Controls	Test Results	Comments	W/P References
1. Changes are authorized.	Obtain a complete list of changes to the IT environment for any high or moderate processes for the fiscal year from July 1st through the date of the test. Select an appropriate sample of changes from the list and determine that the change was appropriately authorized.			
2. Changes are tested.	Obtain a complete list of changes to the IT environment for any high or moderate processes for the fiscal year from July 1st through the date of the test. Select an appropriate sample of changes from the list and determine that the change was appropriately tested.			

3. Changes are approved.	Obtain a complete list of changes to the IT environment for any high or moderate processes for the fiscal year from July 1st through the date of the test. Select an appropriate sample of changes from the list and determine that the change was appropriately approved.			
4. Changes are monitored.	Obtain sufficient evidence to determine that the change process is monitored on a regular basis (e.g., steering committee, management review of changes to production).			
5. Segregation of incompatible duties exits within the manage change environment.	Determine, both organizationally and logically, that different individuals with the agency perform the following duties: • Request/approve program development or program change • Program the development or change • Move programs in and out of production • Monitor program development and changes			

Overall Objective of Logical Access
Only authorized persons have access to data and applications (including programs, tables, and related resources) and that they can perform only specifically authorized functions (e.g., inquire, execute, update).

The objective or the logical access testing related to ITGCs is to confirm there are effective controls in place for adding, updating and deleting user access to financial data and programs and that access to financial data and programs is appropriately restricted. Agency's need to consider whether the ITGC logical access testing gives sufficient evidence regarding the appropriate restriction or segregation of incompatible, relevant accounting duties. In some cases the ITGCs testing may not provide sufficient evidence for one to specifically conclude on whether logical access is appropriately restricted or segregated for individual transactions. This may be the case when access controls at the application level are important to the agency's risk assessments and the conclusion on internal control over financial report. In this situation, agency would perform specific testing on the application level access or segregation of incompatible duties control as part of the application testing.

Logical Access Path
For each application for which agency plans to rely on ITGC's (i.e., those where agencies are relying on application or IT-dependent manual controls or that produce electronic evidence), determine the criticality of each technical component of the logical access path the agency uses to secure access to financial programs and data. The possible technical components of the logical access path include:

- Application
- Operating system, including the security software being used
- Database
- Network
- Internet/Remote Access

To determine the most appropriate testing approach, agency should understand and document the different processes used for managing security. To assist with this, a walkthrough should document where there are different processes for authorizing access along the logical access path. In most environments:

- All of the logical access ITGCs apply at the application level when the controls are important in achieving the control objectives for relevant assertions for significant accounts.
- Not all of the logical access ITGCs apply at the operating system and DBMS levels when the controls are important in achieving the control objectives for relevant assertions for significant accounts.
- Few of the logical access ITGCs likely apply at the network, remote access, or internet levels when the controls are important in achieving the control objectives for relevant assertions for significant accounts.

Complete the Logical Change Table.

Logical Change	Tests of Controls	Test Results	Comments	W/P References
1. General system security settings are appropriate.	Determine that the general system security settings are appropriate based on minimum guidelines defined in our technology-specific guidance, if available.			
2. Password settings are appropriate.	For each relevant technical component of the logical access path, obtain evidence of the agency's settings for the following security configurations: • Minimum password length • Initial log-on uses a onetime password • Password composition (e.g., alpha/numeric characters, not words in dictionary • Frequency of forced password changes • The number of unsuccessful log on attempts allowed before lockout • Ability of users to assign their own passwords • Number of passwords that must be used prior to using a password again • Idle session time out • Logging of unsuccessful login attempts			

3. Access to privileged IT functions is limited to appropriate individuals.	Obtain a list of privileged user rights for the relevant technical components of the logical access path that support the key controls (e.g., users with fully system access or access to security administration functionality). Determine that it is complete. Review the lists of users with privileged rights and determine if the number of users appears appropriate. Based on the volume of users and the critical nature of this control, develop a test to determine if users' privileged access is appropriate based on their job description/functions (this listing should include the review of sensitive system accounts).			
4. Access to system resources and utilities is limited to appropriate individuals.	Identify and obtain a list of resources (e.g., datasets, security, accounting schema, mater files, transactional data), including utilities (e.g., SQL Plus, DFU, Super Zap) associated with the relevant applications that could affect the accuracy of the financial states if not appropriately secured. Determine that access to the resource(s) is appropriate.			

5. User access is authorized and appropriately established.	*Periodic User Validation:* Obtain the periodic validation report(s) and select an appropriate sample to determine that the users' access had been appropriately validated. *New User Setup:* Obtain a list of new users added during the period under review and determine that it is complete. Select an appropriate sample and determine that there was appropriate approval granting the new user access and that the user's access was appropriately established based on his/her job function and the new user request form. *Monitoring of User Access:* Identify relevant monitoring controls and test that the controls functioned as expected over the review period. These controls might include: • Violation or violation attempts reporting and review • Review of logs (i.e., surrounding privileged user access) Determine that system settings are appropriately configured to capture key system events and activities.			

6. Physical access to computer hardware is limited to appropriate individuals	Obtain a list of employees with access to the data center, determine it is complete, and review for appropriateness. Confirm that controls are in place to restrict access to only those individuals.			
7. Logical access process is monitored.	Obtain sufficient evidence to determine that the logical access process is monitored on a regular basis (e.g., monitoring compliance with established logical access control procedures, periodic review of logical access policies and procedures).			
8. Segregation of incompatible duties exists within the logical access environment.	Determine, both organizationally and logically, that different individuals/system resources perform the following duties related to granting user access: • Requesting access, approving access, setting up access, and monitoring access violations/violation attempts • Performing rights of a "privileged" user and monitoring use of a "privileged" user			

Compensating Controls for the User Validation Process

ITGCs related to terminated and transferred users typically are compensating controls for deficiencies with the periodic user access review process (ITGC #5). If the review indicates a need to test terminated and transferred users, agency will need to consider the following procedures:

Logical Change	Tests of Controls	Test Results	Comments	W/P References
1. Terminated Users.	Obtain a list of terminated employees during the review period and determine that it is complete. Select an appropriate sample and determine if system access had been roved or deactivated timely.			
2. Transferred Users.	Obtain a list of transferred employees during the review period and determine that it is complete. Determine if the user's access is appropriate based on his/her job function and his/her previous system access has been removed or deactivated.			

Overall Objective of Other ITGCs

- Backup and Recovery: Data supporting financial information is properly backed-up so such data can be accurately and completely recovered if there is a system outage or data integrity issue.
- Scheduling: Programs are executed as planned and deviations from scheduled processing are identified and resolved in a timely manner.
- Problem and Incident Management and Monitoring: IT operations problems or incidents are identified, resolved, reviewed and analyzed in a timely manner.

Complete Other ITGCs Table.

Other ITGCs	Tests of Controls	Test Results	Comments	W/P References
1. Financial data has been backed-up and is recoverable.	Determine process for identifying date to be backed up. Determine that individuals who perform backups are not also responsible for monitoring them Select an appropriate sample of back-up activity and test that the ITGCs over back-ups are operating as expected. Review the procedures for periodically testing that backups can be restored.			
2. Deviations from scheduled processing are identified and resolved in a timely manner.	Determine that only appropriate users have the ability to make changes to the job schedule and only approved changes are made. Determine that individuals who program/implement /monitor scheduling do not have conflicting duties. Test a sample of errors from production processing. For each, determine that an appropriate level of follow-up and resolution occurred.			

3. IT operations problems or incidents are identified, resolved, reviewed, and analyzed in a timely manner.	Obtain sufficient evidence to determine that IT operations problems or incidents are identified, resolved, reviewed and analyzed in a timely manner.			

Other ITGCs are included when a failure of the related controls could have an effect on the financial statements or disclosures. If controls related to the resolution of deviations from scheduled processing (ITGC #2) are operating effectively, the controls related to reviewing and analyzing problems or incidents (ITGC #3) only require a walkthrough.

APPENDIX 6.1A

FINANCIAL NARRATIVE - EXAMPLE

Fund(s): General Fund

Account(s): Accounts Payable/Expenditures

Significant Process: New Vendor Setup

Significant Process Risk Rating: High

Supporting Systems/Application(s): Application XYZ

This document provides a description of the above Significant Process as of FYE 6/30/20XX. Internal controls are *Italicized*, Critical Controls are **Bolded** and control weaknesses are underlined.

Input *(Beginning of process)* Vendor information (name, address, bank details, payment terms, discounts, matching principal, accounting, etc.)

Output*: (End of process)* Vendor in system

Source(s): Policies and Procedures Manual – Accounts Payable

Prepared by: Name of assessment team member

Interview Date: Jan 1, 20XX

A formal process exists to add or modify vendors. Note that Application XYZ does not permit the deletion of vendors; it will only allow a vendor to be altered or disabled. This process consists of the following activities:

- The Supplier Maintenance Form is filled out by the buyer. This form details the vendor's name, address, bank details, payment terms, discounts, matching principal, accounting information, etc.
- *The form must be signed by the buyer's supervisor, who checks the details for accuracy.* (AP1)
- **The form is then sent to the AP department where it is reviewed and entered into the system.** (AP2)
- *Application XYZ does not allow duplicate supplier names to reside in the system.* (AP3)
- **Vendor maintenance is performed by the AP department and is limited to supervisors. Role-based security is utilized in Application XYZ, such that individuals having access to perform vendor maintenance do not also have access to process invoices and print checks. (AP4)**

APPENDIX 6.1B
COMPLIANCE NARRATIVE

EAGLE Program **Template 02**
Compliance Narrative Template
Agency Name

CFDA Program Title(s) or Cluster:

CFDA #(s):

Supporting System(s) / Application(s):

This document provides a description of the controls in place for the above CFDA Program(s) as of FYE 6/30/20XX. Internal controls are *Italicized*, Critical Controls are **Bolded** and control weaknesses are <u>underlined</u>.

Compliance Requirement(s):

Requirement Risk Rating(s):

Source(s):

Prepared by:

Interview Date:

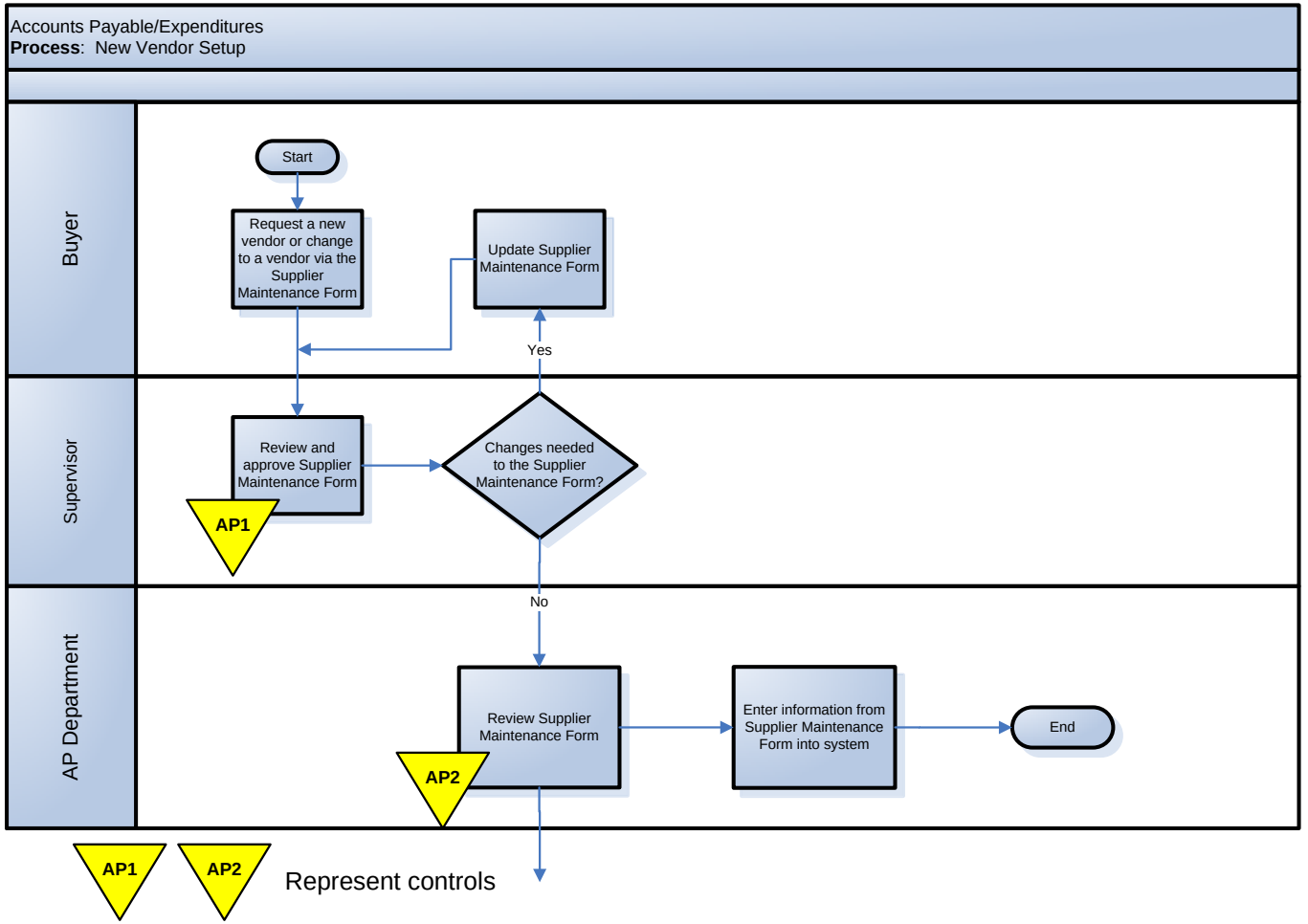
Note: Label all your controls with a control reference number in the above narrative. This control reference number will be cross-referenced throughout the remainder of the templates.

A critical control is a control that will prevent or detect an error in the event that all other controls fail. If there isn't a critical control in the process you may need to test all the controls in your narrative. If the critical control encompasses the prior controls you will only need to test the critical control and not the individual control.

Refer to the Guidance Manual and/or Case Studies for an example of how to complete the narrative template. The narrative should be for the procedures in place at the end of the current fiscal year. If your Agency's procedures are changing during the fiscal year, document the new procedures that will be in effect at the end of the current fiscal year, rather than the old procedures.

APPENDIX 6.3

FLOWCHART EXAMPLE



APPENDIX 6.6A

FINANCIAL RISK AND CONTROL MATRIX

Document:	Risk and Control Matrix (RACM)
Entity:	*Agency Name*
Reporting Date:	June 30, 20XX
Fund:	General Fund
Financial Statement Account(s):	Accounts Payable/Expenditures
Systems / Applications:	Application XYZ

Prepared by:	T.Smith
Reviewed by:	J. Doe

Significant Process	Process Risk Rating	Financial Statement Assertions	Risks	Control Owner	Control Description	Control Ref. #	Automated, Manual or Both?	Prevent or Detect?	Frequency of Control Activity
New Vendor Setup	High	Existence; Rights & Obligations	Unauthorized or incorrect changes are made to the vendor master file, increasing the risk of fraudulent payment transactions.	Supervisor	The Supplier Maintenance Form is reviewed and approved by the buyer's Supervisor.	**AP1**	Manual	Prevent	More than daily
				AP Department	The Supplier Maintenance Form is sent to the AP department where it is reviewed and entered into the system.	**AP2**	Manual	Prevent	More than daily
				Application XYZ	Application XYZ does not allow duplicate supplier names to reside in the system.	**AP3**	Automated	Prevent	Continuous
				Application XYZ	Vendor maintenance is performed by the AP department and is limited to supervisors. Role-based security is utilized in Application XYZ, such that individuals having access to perform vendor maintenance do not also have access to process invoices and print checks.	**AP4**	Automated	Prevent	Continuous

APPENDIX 6.6B

COMPLIANCE RISK AND CONTROL MATRIX

EAGLE Program

Document:	Risk and Control Matrix (RACM)
Entity:	*Agency Name*
Reporting Date:	*June 30, 20XX*
CFDA Program Title(s) or Cluster:	
CFDA #(s):	
Systems / Application(s):	

Prepared by:	
Reviewed by:	

Compliance Requirement(s)	Requirement Risk Rating(s)	Risks	Control Owner	Control Description	Control Ref. #	Automated, Manual or Both?	Prevent or Detect?	Frequency of Control Activity

APPENDIX 6.8A

FINANCIAL WALKTHROUGH - EXAMPLE

Fund(s): General Fund
Account(s): Accounts Payable/Expenditures
Significant Process: New Vendor Setup
Significant Process Risk Rating: High
Supporting System(s)/Application(s): Application XYZ

This walkthrough assists in documenting our understanding of the design of controls. We are documenting the procedures performed, evidence obtained and conclusions as to the effective design of the underlying controls and whether the controls have been implemented. We will select a transaction that has occurred within the current Fiscal Year and walkthrough all controls listed on the narrative template (template 02).

Walkthroughs should be performed by someone who is not ordinarily involved in the process, and if possible, should be performed when the process occurs. A walkthrough should be performed for all controls identified in the narrative, both critical and non-critical.

Control Owner's Title: AP Buyer
Date of Walkthrough/Interview: January 1, 20XX
Walkthrough performed by: Jane Smith

Control Description and Control Reference #: *The Supplier Maintenance Form must be signed by the buyer's supervisor, who checks the details for accuracy. (AP1)*

Transaction Selection: South Telephone (Vendor #100)

Procedures to Perform: We obtained the Supplier Maintenance Form for South Telephone vendor and verified the supervisor's approval.

Results: We noted that all the Supplier Maintenance Form details were filled out and the form was approved by the buyer's supervisor (refer to w/p AP1.1).

Conclusion: The control was in place and operating effectively at the time of the walkthrough.

Control Description and Control Reference #: The Supplier Maintenance Form is then sent to the AP department where it is reviewed and entered into the system. (AP2)

Transaction Selection: South Telephone (Vendor #100)

Procedures to Perform: We obtained the Supplier Maintenance Form and verified the information was entered correctly into the system.

Results: We noted that the form details including the vendor's name, address, bank details, payment terms, and discounts agreed to the system (refer to w/p AP1.2).

Conclusion: The control was in place and operating effectively at the time of the walkthrough.

FINANCIAL WALKTHROUGH EXAMPLE (CONTINUED)

Control Description and Control Reference #: *Application XYZ does not allow duplicate supplier names to reside in the system. (AP3)*

Transaction Selection: South Telephone (Vendor #100)

Procedures to Perform: We tested the system for duplicate entry of supplier names.

Results: We obtained a Supplier List Report from the system and noted that our selected vendor, South Telephone, resides within the system. We requested that the Buyer enter the same vendor name into the system. We noted that the system appropriately rejected the vendor (refer to w/p AP1.3).

Conclusion: The control was in place and operating effectively at the time of the walkthrough.

Control Description and Control Reference #: Vendor maintenance is performed by the AP department and is limited to supervisors. Role-based security is utilized in Application XYZ, such that individuals having access to perform vendor maintenance do not also have access to process invoices and print checks. (AP4)

Transaction Selection: AP Supervisor E. Jones and N. Taylor

Procedures to Perform: We obtained a list of employees by department from Human Resources and the list of Application XYZ user access rights for all AP functions to determine if proper segregation of duties exists.

Results: We verified that access rights for AP functions are limited to the AP department. We then reviewed the access rights for E. Jones and N. Taylor. We noted that they had access rights to vendor maintenance as well as other AP functions, such as process invoices and print checks. This is a segregation of duties issue (refer to w/p AP1.4).

Conclusion: The control is ineffective. See Issue Summary Log for additional details of the exception.

APPENDIX 6.8B
COMPLIANCE WALKTHROUGH

EAGLE Program **Template 03**
Compliance Walkthrough Template
Agency Name

CFDA Program Title(s) or Cluster:
CFDA #(s):
Compliance Requirement:
Requirement Risk Rating:
Supporting System(s)/Application(s):

This walkthrough assists in documenting our understanding of the design of controls. We are documenting the procedures performed, evidence obtained and conclusions as to the effective design of the underlying controls and whether the controls have been implemented. Select a transaction that has occurred within the current Fiscal Year and walk through all controls listed on the narrative template (template 02).

Control Owner's Title:
Date of Walkthrough/Interview:
Walkthrough Performed by:

Control Description and Control Reference #:

Transaction Selection:

Procedures to Perform:

Results:

Conclusion:

Note: This walkthrough will assist you when the test of controls is performed. During the walkthrough, if a control does not appear to be in place for the item selected, look at a few additional items to determine if the error noted for the first item was an isolated incident. If the issue is recurring, it is not necessary to document a test plan and perform testing. The issue should be added to the Issue Summary Log.

Refer to Guidance Manual and/or Case Studies for an example of how to complete the walkthrough template.

APPENDIX 6.9

North Carolina
EAGLE Program
Service Provider Inventory Template

Agency:	
Financial Statement Date:	FYE June 30, 20XX
Date Assessment Performed:	
Assessment Performed By:	

Purpose:	The purpose of this form is to document the central management agencies and third-party service organizations that are used to support the various business processes for the specified agency.

During the documentation phase of EAGLE, the assessment team will use this form to identify the significant processes performed by service providers. **This form should only be completed if your agency relies on processes and controls performed by service providers. If no reliance is placed on service providers, then your agency should have controls documented in your narrative that eliminate the need to rely on controls outside of your agency.**

A **service provider** is defined as an organization that performs services on behalf of another entity. When an agency uses a **service provider**, transaction processes that impact the agency's financial statements are subjected to controls that are, at least in part, physically and operationally separate from the agency. For state agencies, service providers can be either central management service agencies or third-party service organizations.

Central management agencies include the following:

- Department of State Treasurer (DST),
- Office of Information Technology Services (ITS),
- Office of State Budget and Management (OSBM),
- Office of the State Controller (OSC),
- Department of Administration (DOA), and
- Community College System Office.

Core banking (DST), information system support (ITS), and payroll processing (OSC) are all examples of services performed by central management agencies.

Third-party service organizations are external providers that perform specific tasks or replace entire business units or functions of an agency. Third-party service organizations may:

- Execute transactions and/or maintain accountability for agencies, or
- Record transactions and process related data for agencies.

BlueCross BlueShield, which processes claims on behalf of the State Health Plan, is an example of a third-party service organization. Fidelity Investment Manager, which manages the investment portfolio on behalf of the College, is another example.

Instructions for completing the Inventory Template

Significant Process	List all significant processes performed by a service provider.
Service Provider	Identify the service provider.
Service Type	Identify if the service provider is a central management agency or third-party service organization.
SOC 1 and/or 2, Type 2 available?	Indicate if a SOC 1 and/or SOC 2, Type 2 report is available for the service provider. **SOC 1, Type 2** reports describe controls and indicate if those controls have been placed into operation. This is not enough to meet the requirements of the EAGLE program. **SOC 2, Type 2** reports go one step further by testing the operating effectiveness of controls. If you answer 'yes' to this question, complete Reliance on the Work of Others Template.
Additional Information	Provide an explanation if you answered 'no' to the above question. This column may also be used to document any other information that may assist in your review and evaluation of service provider controls.

Service Provider Inventory Template				
Significant Process	**Service Provider**	**Service Type**	**SOC 1 and/or 2, Type 2 available?**	**Additional Information**
Process payroll	OSC - BEACON	Central Mgmt	No	Not available at this time.
Post to G/L	OSC - NCAS	Central Mgmt	No	Not available at this time.
Claims Adjustment	BCBS	Third-Party	Yes	SOC 2, Type 2
Colleague program changes	NCCCS	Central Mgmt	No	Not available at this time.
Determining the fair value of the investment portfolio	Fidelity Investment Manager	Third-Party	Yes	SOC 1, Type 2 as of June 30, 20XX

Conclusion: In the Risk Assessment Template 01, we identified significant accounts and related significant processes. These significant processes are where transactions are initiated, recorded, processed and/or reported. For the significant processes performed by another entity, we have identified the service provider and noted the availability of a SOC 1 and/or SOC 2, Type 2 report.

APPENDIX 6.9

RELIANCE ON THE WORK OF OTHERS TEMPLATE

Agency:	
Financial Statement Date:	FYE June 30, 20XX
Date Assessment Performed:	
Assessment Performed By:	

Service Provider:	

Purpose:	The purpose of this form is to document the review of the service provider's SOC 1 or SOC 2, Type 2 report.

In the Service Provider Inventory Template above, we identified the significant processes performed by service providers. Using this form, we will review and evaluate the service provider's controls over the significant processes.

Instructions

If you have a SOC 1 or SOC 2, Type 2 report from a service provider (central management agency or third-party service organization), please complete the following questions.

If a SOC 1 or SOC 2, Type 2 report is not available, contact Risk Mitigation Services for further guidance at (919) 707-0795 or e-mail us at OSC.EagleSupport@lists.osc.nc.gov.

1. Agencies need to evaluate the service provider's information and its adequacy in addressing the flow of information, the design of the processing procedures and controls at the service provider, and any tests of the operating effectiveness of those controls that in effect represent a component of the agency's overall system of internal control over financial reporting. We need to consider whether these results provide sufficient evidence to support their internal control environment.

   Evaluate and describe the service provider's results.

		Yes	No
a.	Is there sufficient documentation of processes, utilizing policies, procedures, narratives, and flowcharts, such that the agency can understand the relevant processes at the service provider along with the flow of transactions through the service provider? Have relevant risks been identified?	☐	☐

If no, describe what is missing.

b. Are the service provider's relevant controls documented? ☐ ☐

c. Does the control documentation describe in sufficient detail the controls that have been implemented to prevent or detect those possible risks, and do the controls appear to be suitably designed to meet those objectives? ☐ ☐

d. Is there testing evidence (walkthroughs, testing sheets) to support the design and operating effectiveness of the defined controls? ☐ ☐

e. Has the nature of any noted exceptions been adequately described? ☐ ☐

Describe exceptions.

If, after review of the service provider's results, we conclude that additional evidence about the operating effectiveness of controls at the service provider is required, we will need to consider other potential sources of information, such as policies and procedures, processing descriptions, and manuals to gain the needed understanding of the controls at the service provider, which may include:

- Evaluating the procedures performed by management and the results of those procedures.
- Contacting the service provider to obtain specific information.
- Requesting that additional documentation and testing be conducted to supply the necessary information.

Describe the additional procedures performed, if applicable.

Conclusion

	Yes	No
Do we have a sufficient understanding of the effect of the service provider on the agency's internal control over financial reporting, including an understanding of the controls placed in operation by the service provider whose services are part of the agency's information system?	☐	☐

Is the control testing performed by the service provider relevant to and sufficient for purposes of our assessment of internal control over financial reporting?	☐	☐

Describe any additional procedures that need to be performed.

APPENDIX 7.1

DETERMINING FACTORS FOR SAMPLE SIZE	
Variability of the Population	The variability of the population has a direct effect on the required sample size. As variability (measured as the standard deviation of the population in statistical sampling) increases, the required sample size increases significantly. For highly variable populations, we generally stratify the population into two or more ranges, each of which represents a less diverse population which can be independently sampled. For tests of controls and monetary unit sampling, variability is addressed through an **expected error rate.**
Expected Error Rate	The expected error rate reflects the tester's assessment of the *probable* rate of noncompliance or amount of error. It is used for tests of controls that use monetary unit sampling. An estimate of the expected amount of error in a particular account balance or group of transactions is based on the following factors: • Understanding of the entity's business • Prior years' tests of the population • Results derived from a small pilot sample
Desired Reliability Level	In determining an acceptable level of risk, the Tester should consider the degree of audit risk that is appropriate and the reliance that can be placed on the internal control structure and other audit procedures. In statistical sampling, this is expressed as a **reliability** or **confidence level** that the results will provide correct information about the whole population. Reliability or confidence levels in the range of 90%-95% would be typical for many audit tests.
Tolerable Error Rate	The tolerable error is an estimate of the maximum rate of noncompliance or level of error that the Tester is willing to accept in an account balance or group of transactions. Viewed from a different perspective, it is the potential error rate that a given sample is designed to detect with a given level of confidence. Lower tolerable error requires larger sample sizes, all other things being equal.
Population Size	Although sample sizes increase for larger populations, the increase is not proportional and, for large populations (>5000 units), the impact is negligible. For example, all other factors held constant, if a population of 1000 required a statistical sample of 85, a population of 50 would require a sample of 33 and a population of 100,000 would require a sample of 93.

APPENDIX 7.2

SAMPLE SIZE GUIDANCE TABLE

Below is the recommended sample size table to be used based on level of risk:

Estimated Population	Frequency of Control	Range of Sample Size	Process Risk		
			Low	Moderate	High
More than 250	More than daily/ Continuous	25	25	25*	25**
61-249	Daily	15-25	15	20	25
40-60	Weekly	5-10	5	7	10
20-39	Bi-Weekly/ Semi-Monthly	3-7	3	5	7
12-19	Monthly	2-4	2	3	4
4-11	Quarterly	2	2	2	2
1-3	Annually	1	1	1	1
N/A	Automated	1	1	3	4

Note 1: The risk assessment of a specific process is based on the judgment of the tester and is a function of the process' level of complexity, routineness, centralization, and automation.

Note 2: For controls with a frequency of "As needed" or "Event Based", use the "Range of Sample Size" guidance above that is closest to the estimated population. For example, if a control occurs as needed and the actual or estimated population equals 45 occurrences, then our sample size guidance indicates we should follow the "Weekly" frequency which is the closest estimated population size noted above.

* - During the test of controls, if a weakness of control is identified (i.e.; an exception is noted), you must expand your test sample from 25 to 30. By doing so, you will determine whether this exception was an isolated incident or a weakness of control.

** - During the test of controls, if a weakness of control is identified (i.e.; an exception is noted), you must expand your test sample from 25 to 40. By doing so, you will determine whether this exception was an isolated incident or a weakness of control.

APPENDIX 7.3A
FINANCIAL TEST PLAN

Document:	Test Plan
Entity:	*Agency Name*
Reporting Date:	June 30, 20XX
Fund:	General Fund
Financial Statement Account(s):	Accounts Payable/Expenditures

Prepared by:	T. Smith
Reviewed by:	J. Doe

						Complete after testing			
Significant Process	**Process Risk Rating**	**Control Description**	**Control Ref. #**	**Objective of Test**	**Testing Procedures**	**Results**	**Conclusion**	**Issue Raised?**	**Testing w/p ref**
New Vendor Setup	High	Vendor maintenance is performed by the AP department and is limited to supervisors. Role-based security is utilized in Application XYZ, such that individuals having access to perform vendor maintenance do not also have access to process invoices and print checks.	*AP4*	Ensure that only authorized personnel (AP Supervisors) have access rights to perform vendor maintenance.	In order to verify appropriate access rights for vendor maintenance, compare Application XYZ access rights for employees to the HR listing of AP employees.	*Exceptions noted.*	*Ineffective*	*Yes*	*P2P.Testing Leadsheet; Issue Summary Log*

APPENDIX 7.3B
COMPLIANCE TEST PLAN

EAGLE Program

Document:	Test Plan
Entity:	*Agency Name*
Reporting Date:	June 30, 20XX
CFDA Program Title(s) or Cluster:	
CFDA #(s):	

Prepared by:	
Reviewed by:	

						Complete after testing			
Compliance Requirement(s)	**Requirement Risk Rating**	**Control Description**	**Control Ref. #**	**Objective of Test**	**Test Procedures**	**Results**	**Conclusion**	**Issue Raised?**	**Test W/P Ref.**
							<Select Answer>	<Select Answer>	
							<Select Answer>	<Select Answer>	
							<Select Answer>	<Select Answer>	
							<Select Answer>	<Select Answer>	

APPENDIX 7.4A
FINANCIAL TEST LEADSHEET

EAGLE Program

Document:	Test Leadsheet
Entity:	*Agency Name*
Reporting Date:	June 30, 20XX
Fund:	General Fund
Financial Statement Account(s):	Accounts Payable/Expenditures

Performed by:	T. Smith
Reviewed by:	J. Doe

Significant Process:	New Vendor Set-up	The process in which the control resides.
Process Risk Rating:	High	The risk ranking associated with the process based on the risk assessment.
Control Reference #:	AP4	
Control Description:	Vendor maintenance is performed by the AP department and is limited to supervisors. Role-based security is utilized in Application XYZ, such that individuals having access to perform vendor maintenance do not also have access to process invoices and print checks.	
Control Frequency:	Continuous	How often the control is performed (i.e., daily, weekly, monthly, etc.)
Automated, Manual or Both:	Automated	Automated, Manual, or IT-dependent
Prevent or Detect:	Prevent	
Control Owner:	AP Supervisor	The person responsible for performing the control.
Estimated Population:	24	Total population for process being tested.
Sample Selection Methodology:	Random	How the sample was selected (i.e., random, judgmental, haphazard, etc.)
Sample Size:	7	Number of items selected based on Sample Size Guidance Table.
Source Test Documents:	List of all AP department employees; List of user access rights for Application XYZ vendor maintenance function.	Documentation obtained as evidence for testing.
Testing Procedures:	We obtained a list of all AP employees with vendor maintenance access rights. We then determined if access was appropriate based on their role.	Explain how the sample was selected and state procedures performed during testing.
Definition of an Exception:	Employee is not an AP Supervisor; Employee does not have appropriate access rights based on his/her role.	The condition in place when a control is not met. Define exceptions before testing.

Testing Section:	Customize column headings as necessary			**Attributes**		
Sample No.	**Employee ID#**			**A**	**B**	**W/P Ref.**
1	2586598			Y	Y	
2	2214543			N	N	P2P
3	2446942			N	N	P2P
4	3654782			N	N	P2P
5	3874215			N	N	P2P
6	2987432			Y	N, Note 1	P2P
7	3154987			N	N	P2P

The header fields in gray should be customized for the items you are testing. Add columns as necessary.

List each sample item selected and indicate if each attribute was satisfied or not. Add rows as necessary.

Attributes:	**A**	Employee is an AP Supervisor.
	B	Employee has appropriate access rights based on his/her role.

List each attribute that was tested. An attribute is a characteristic that either exists or does not exist.

Tickmark Legend:	**Y**	Attribute satisfied without exception.
	N	Attribute not satisfied.
	Note 1	Supervisor has access to all AP functions.

Explain tickmarks used in the testing matrix above.

Results:	In our sample, 6 of 7 AP employees have inappropriate access rights; 5 of the 7 have access to vendor maintenance but are not AP Supervisors. This has been discussed with management and will be included on the Issue Summary Log.

Summarize the results of testing. Note any exceptions and describe any observations.

APPENDIX 7.4B
COMPLIANCE TEST LEADSHEET

EAGLE Program

Document:	Test Leadsheet
Entity:	*Agency Name*
Reporting Date:	June 30, 20XX
CFDA Program Title(s) or Cluster:	
CFDA #(s):	

Performed by:	
Reviewed by:	

Compliance Requirement(s):	
Requirement Risk Rating:	
Control Reference #:	
Control Description:	
Control Frequency:	
Automated, Manual or Both:	
Prevent or Detect:	
Control Owner:	
Estimated Population:	
Sample Selection Methodology:	
Sample Size:	
Source Test Documents:	
Test Procedures:	
Definition of an Exception:	

Testing Section:	Customize column headings as necessary				**Attributes**		
Sample No.	**Invoice No.**	**Vendor**	**Date**	**etc.**	**A**	**B**	**W/P Ref.**

Attributes:	**A**	
	B	
Tickmark Legend:		
Results:		

APPENDIX 7.6A
FINANCIAL ISSUE SUMMARY LOG

Prepared by:	T. Smith
Reviewed by (ICO and CFO):	J. Doe

Agency Name
Issue Summary Log
June 30, 20XX

Financial Statement Account(s)	Significant Process	Process Risk Rating	Control Description	Control Ref #	Issue	Risk/Implication	Recommendation	Management's Response
Accounts Payable/ Expenditures	New Vendor Set-Up	High	Vendor maintenance is performed by the AP department and is limited to supervisors. Role-based security is utilized in Application XYZ, such that individuals having access to perform vendor maintenance do not also have access to process invoices and print checks.	AP4	To verify our understanding of the process, we obtained the list of Application XYZ user access rights for all AP functions. We noted 2 supervisors that had access rights to vendor maintenance as well as other AP functions, such as process invoices and print checks. This is a segregation of duties issue. We further tested a sample of 7 AP employees with vendor maintenance rights. Five of the employees were not supervisors; one of the supervisors had access to process invoices and print checks.	Unauthorized or incorrect changes are made to the vendor master file, increasing the risk of fraudulent payment transactions.	We recommend that management review the AP user access rights in detail to help ensure that access to perform vendor maintenance is restricted to only AP supervisors. Additionally, we recommend that those supervisors are restricted from performing other AP functions, such as processing invoices and printing checks.	Access rights for vendor maintenance will immediately be restricted to AP supervisors only. Additionally, the Controller will perform a segregation of duties review to further restrict access within the AP department.

APPENDIX 7.6B
COMPLIANCE ISSUE SUMMARY LOG

Prepared by:	
Reviewed by (ICO and CFO):	

EAGLE Program
Issue Summary Log
Agency Name
June 30, 20XX

CFDA Program Title(s) or Cluster	Compliance Requirement(s)	Requirement Risk Rating	Control Description	Control Ref. #	Issue	Risk/Implication	Recommendation	Management's Response

APPENDIX 8.2A
PERFORMANCE – GENERAL ACCOUNTING

Auto Calculating Field
Data Entry Field
Benchmark should be determined by Agency
Low Risk
Moderate Risk
High Risk

KEY PERFORMANCE INDICATORS SUMMARY

Agency Name: General Accounting

Prepared by:

Reviewed by:

Reported Fiscal Year: 2011/2012

ID #	General Accounting KPIs	Frequency	2011 Jul	2011 Aug	2011 Sep	2011 Oct	2011 Nov	2011 Dec	2012 Jan	2012 Feb	2012 Mar	2012 Apr	2012 May	2012 Jun	2012 Jul	2012 Aug	2012 Sep	Comments	Benchmark: Goal	Green Range	Yellow Range	Red Range
	Month-End Activities																					
GA01	*Average # of Business Days to Reconcile Bank Accounts*	Monthly																	15 Business Days	1-15 Business Days	16-30 Business Days	>30 Business Days
GA02	*Average # of Business Days to Resolve Bank Account Reconciliation Discrepancies*	Monthly																	40 Business Days	1-40 Business Days	41-60 Business Days	>60 Business Days
GA03	*# of Business Days to Certify NCAS Balances*	Monthly																	10 Business Days	1-10 Business Days	11-15 Business Days	>15 Business Days
	Year-End Activities																					
GA04	*# of Calendar Days to Submit the Certification of Internal Controls*	Annually																	31 Calendar Days	31 Calendar Days	32-58 Calendar Days	>58 Calendar Days
GA05	*# of Calendar Days to Submit and Certify CAFR Package*	Annually																	60 Calendar Days	1-60 Calendar Days	61-67 Calendar Days	>67 Calendar Days
GA06	*# of Calendar Days to Complete Annual Financial Statements Notes (UNC-H only)*	Annually																	92 Calendar Days	1-92 Calendar Days	93-122 Calendar Days	>122 Calendar Days
GA07	*Current Ratio Calculation (UNC-H Only)*	Annually																	Benchmark should be determined by Agency			
	Risk Assessment Activities																					
GA08	*# of High Risk Internal Control Issues Identified and Documented*	Annually																	0 Issues	0 Issues	1-5 Issues	>5 Issues
GA09	*# of Moderate Risk Internal Control Issues Identified and Documented*	Annually																	0 Issues	0 Issues	1-5 Issues	>5 Issues
	Audit Findings																					
GA10	*# of Financial Statement Audit Findings*	Annually																	0 Audit Findings	0 Audit Findings	1-3 Audit Findings	>3 Audit Findings
GA11	*# of Resolved Financial Statement Audit Findings*	Annually																	Data used for the below benchmark calculation.			
GA12	*% of Resolved Financial Statement Audit Findings*	Annually																	100%	100%	90-99%	<90%
GA13	*# of Fiscal Control Audit Findings*	Annually																	0 Audit Findings	0 Audit Findings	1-3 Audit Findings	>3 Audit Findings
GA14	*# of Resolved Fiscal Control Audit Findings*	Annually																	Data used for the below benchmark calculation.			
GA15	*% of Resolved Fiscal Control Audit Findings*	Annually																	100%	100%	90-99%	<90%

APPENDIX 8.2B
PERFORMANCE – FEDERAL GRANTS

Auto Calculating Field
Data Entry Field
Benchmark should be determined by Agency
Low Risk
Moderate Risk
High Risk

KEY PERFORMANCE INDICATORS SUMMARY

Agency Name
Federal Grants

Prepared by:
Reviewed by:

Reported Fiscal Year: 2011/2012

ID #	Federal Grants KPIs	Frequency	2011 Jul	Aug	Sep	Oct	Nov	Dec	2012 Jan	Feb	Mar	Apr	May	Jun	Comment	Benchmark Goal	Green Range	Yellow Range	Red Range
	Compliance with Grant Requirements																		
FG01	*# of Federal Audit Findings*	Quarterly														0	0	1-3	3+
FG02	*# of State Audit Findings*	Quarterly														0	0	1-3	3+
FG03	*# of Resolved Findings (Federal and State)*	Quarterly														Data used for the below benchmark calculation.			
FG04	*% of Resolved Findings (Federal and State)*	Quarterly														100%	100%	80-99%	<80%
	Timeliness of Reporting																		
FG05	*# of Required Federal Reports*	Quarterly														Data used for the below benchmark calculation.			
FG06	*# of Federal Reports Submitted Within Established Timeframe*	Quarterly														Data used for the below benchmark calculation.			
FG07	*% of Federal Reports Submitted Within Established Timeframe*	Quarterly														100%	100%	95-99%	<95%
FG08	*# of Business Days Late*	Quarterly														0	0	1-20	20+
	Compliance with Monitoring Requirements																		
FG09	*# of Subrecipients Receiving Federal Awards*	Annually														Data used for the below benchmark calculation.			
FG10	*# of Award Letters Sent to Subrecipients Within Established Timeframe*	Annually														Data used for the below benchmark calculation.			
FG11	*% of Award Letters Sent to Subrecipients Within Established Timeframe*	Annually														100%	100%	90-99%	<90%
FG12	*# of Subrecipients Assessed as High Risk*	Annually														Data used for the below benchmark calculation.			
FG13	*# of High Risk Subrecipients Monitored During the Reporting Period*	Annually														Data used for the below benchmark calculation.			
FG14	*% of High Risk Subrecipients Monitored During the Reporting Period*	Annually														100%	95-100%	85-94%	<85%
	Efficiency of Monitoring																		
FG15	*# of Employees Assigned to Subrecipient Monitoring*	Annually														Data used for the below benchmark calculation.			
FG16	*# of Desk Reviews Performed on Subrecipients*	Annually														Data used for the below benchmark calculation.			
FG17	*# of Site Visits to Subrecipients*	Annually														Data used for the below benchmark calculation.			
FG18	*Ratio of Desk Reviews to Employees*	Annually														Benchmark should be determined by Agency			
FG19	*Ratio of Site Visits to Employees*	Annually														Benchmark should be determined by Agency			
	Timeliness of A-133 Audit Report Review & Follow Up																		
FG20	*# of Subrecipients Required to Submit Audit Reports*	Annually														Data used for the below benchmark calculation.			
FG21	*# of Subrecipient Audit Reports Received and Reviewed Within Established Timeframe*	Annually														Data used for the below benchmark calculation.			
FG22	*% of Subrecipient Audit Reports Received and Reviewed Within Established Timeframe*	Annually														100%	90-100%	75-89%	<75%
FG23	*# of Subrecipient Audit Reports with Findings Requiring Management Response Within 6 Months of Receipt of Report*	Annually														Data used for the below benchmark calculation.			
FG24	*# of Mangement Responses Issued Within 6 Months of Receipt of Audit Report*	Annually														Data used for the below benchmark calculation.			
FG25	*% of Mangement Responses Issued Within 6 Months of Receipt of Audit Report*	Annually														100%	100%	90-99%	<90%

APPENDIX 8.2C
PERFORMANCE – PROCUREMENT

KEY PERFORMANCE INDICATORS SUMMARY

Agency Name	*Prepared by:*
Procurement	*Reviewed by:*
	Reported Fiscal Year: 2011/2012

Auto Calculating Field
Data Entry Field
Benchmark should be determined by Agency
Low Risk
Moderate Risk
High Risk

ID #	Procurement KPIs	Frequency	2011 Jul	Aug	Sep	Oct	Nov	Dec	2012 Jan	Feb	Mar	Apr	May	Jun	Comments	Benchmark Goal	Green Range	Yellow Range	Red Range
	Compliance with P&C Rules and Regulations																		
P01	*# of Training Sessions per Employee*	Annually														Data used for the below benchmark calculation.			
P02	*# of P&C Compliance Findings/Issues*	Annually														0	0	1-3	>3
P03	*# of Resolved P&C Compliance Findings/Issues*	Annually														Data used for the below benchmark calculation.			
P04	*% of Resolved P&C Compliance Findings/Issues*	Annually														100%	100%	90-99%	<90%
P05	*Ratio of Training Sessions per Employee to Compliance Findings/Issues*	Annually														Benchmark should be determined by Agency			
	Efficiency in Using E-Commerce																		
P06	*# of AP Vouchers Processed*	Monthly														Data used for the below benchmark calculation.			
P07	*# of ACH Transactions*	Monthly														Data used for the below benchmark calculation.			
P08	*# of P-Card Transactions*	Monthly														Data used for the below benchmark calculation.			
P09	*% of AP Transactions Processed by P-Card or ACH Payments*	Monthly														Benchmark should be determined by Agency			

APPENDIX 8.2D
PERFORMANCE – STUDENT FINANCIAL AID

Auto Calculating Field
Data Entry Field
Benchmark should be determined by College
Low Risk
Moderate Risk
High Risk

KEY PERFORMANCE INDICATORS SUMMARY

Community College Name

Student Financial Aid

Prepared by:

Reviewed by:

Reported Fiscal Year: 2011/2012

ID #	Financial Aid KPIs	Frequency	2011 Jul	2011 Aug	2011 Sep	2011 Oct	2011 Nov	2011 Dec	2012 Jan	2012 Feb	2012 Mar	2012 Apr	2012 May	2012 Jun	2012 Jul	2012 Aug	2012 Sep	Comments	Benchmark Goal	Benchmark Green Range	Benchmark Yellow Range	Benchmark Red Range
	Timeliness of Loan Disbursements																					
FA01	*$ Total Electronic Funds transfer (EFT) Loan Amounts Received*	Monthly																	Data used for the below benchmark calculation.			
FA02	*$ Total EFT Loan Amounts Not Disbursed Within X Business Days*	Monthly																	Data used for the below benchmark calculation.			
FA03	*% of EFT Loan Amounts Disbursed Within X Business Days*	Monthly																	100%	100%	98%-100%	<98%
	Ability to Identify and Follow Up with Students																					
FA04	*# of Title IV Recipients*	Annually																	Data used for the below benchmark calculation.			
FA05	*# of Students Receiving Title IV Aid Who Were Initially Determined SAP (Satisfactory Academic Progress) Non-Compliant*	Annually																	Data used for the below benchmark calculations			
FA06	*% of Students Receiving Title IV Aid Who Were Initially Determined SAP Non-Compliant*	Annually																	Benchmark should be determined by College			
FA07	*# of Students Who Appealed SAP Noncompliance*	Annually																	Data used for the below benchmark calculations			
FA08	*% of Students Who Appealed SAP Noncompliance*	Annually																	Benchmark should be determined by College			
FA09	*# of Students' Appeals Approved*	Annually																	Data used for the below benchmark calculation.			
FA10	*% of Students' Appeals Approved*	Annually																	Benchmark should be determined by College			
	Exit Counseling																					
FA11	*# of Students with Federal Loan History Who Graduated, Withdrew or Dropped Below Half-Time*	Semesterly																	Data used for the below benchmark calculation.			
FA12	*# of Students with Federal Loan History Notified of Exit Counseling Within 30 Days of Graduating, Withdrawing, or Dropping Below Half-Time*	Semesterly																	Data used for the below benchmark calculation.			
FA13	*% of Students with Federal Loan History Notified of Exit Counseling Within 30 Days of Graduating, Withdrawing or Dropping Below Half-Time*	Semesterly																	100%	100%	98%-100%	<98%